Digital governance in support of infrastructure asset management

Bekker, Martinus Jacobus

Digital Governance In Support Of Infrastructure Asset Management

Thinus Bekker

Digital Governance In Support Of Infrastructure Asset Management

Publisher: University of Groningen

Groningen, the Netherlands

Printed by: IpskampDrukkers B.V.

Enschede, The Netherlands

ISBN: 978-90-367-8700-0 (Book)
978-90-367-8699-7 (Electronic version)

Marthinus Jacobus Bekker

Digital Governance in Support of Infrastructure Asset Management

Doctoral Dissertation, University of Groningen, the Netherlands

Keywords: digital governance, IT governance, infrastructure asset management, decision making, design science, information management, enterprise architecture, transition management, information technology, control systems, digital technology.

university of groningen

Digital Governance In Support Of Infrastructure Asset Management

Proefschrift

ter verkrijging van de graad van doctor aan de
Rijksuniversiteit Groningen
op gezag van de
rector magnificus prof. dr. E. Sterken
en volgens besluit van het College voor Promoties.

De openbare verdediging zal plaatvinden op

donderdag 24 maart 2016 om 12:45 uur

door

Marthinus Jacobus Bekker
geboren op 6 februari 1967
in Tzaneen, Zuid Afrika

Promotor

Prof. dr. H.G. Sol

Beoordelingscommissie

Prof. dr. E.W. Berghout

Prof. dr. ir. H.W.G.M. van Heck

Prof. dr. P.M.A. Ribbers

Preface and Acknowledgements

This research was born from a business need of Rand Water, a South African regional bulk water utility, to make evidence-based strategic infrastructure asset management decisions, by considering relevant asset information from both the IT systems and control systems. A number of problems were identified that could prevent the successful enablement and support of infrastructure asset management decision making in a sustained manner. A new way of infrastructure asset information management and digital governance was required, in order to resolve these problems. An appropriate approach was also required to implement the new way of thinking and working in a sustainable manner for a large, complex heterogeneous organisation, such as Rand Water.

In this dissertation an appropriate enterprise-wide integrated digital governance approach for any infrastructure asset intensive organisation is defined that adds value to the organisation, mitigate the related risks, and includes IT and control system environments. The appropriate transition management approach is also defined that will successfully implement the new way of thinking and working in a sustainable way for all digital functions of any large, complex and heterogeneous infrastructure asset intensive organisation. The PhD research, of which this dissertation is the outcome, was conducted from September 2013 to September 2015. It aims to make a contribution to the fields of digital information management and digital governance, especially for infrastructure asset intensive organisations. The researcher is a reflective practitioner fulfilling the role of the Chief Information Officer at Rand Water.

Attaining a PhD has been a life-long ambition. It has been a long, but gratifying and worthwhile, journey. I am indebted to everyone who supported me during this journey. My sincere gratitude goes to my promoter, Professor Henk Sol, for his tireless guidance, encouragement, passion, dedication and patience throughout this journey. A special thanks to my colleagues at Rand Water for assisting in the instantiation and evaluation of the artefact. I'm also grateful to my fellow CIOs at other organisations who took the time and made the effort to evaluate the artefact. I'm further grateful to the Rand Water Group Shared Services Executive, Dr. Fawcett Ngoatje, for encouraging me to pursue a PhD and for granting me approval to use Rand Water as the base case for this research. A special thanks to Les Lange who introduced me to Professor Sol and his PhD school. To my wife, Antonet, and my son,

Martin, thank you for the endless support, prayers, motivation and sacrifices. Thank you to the rest of my family for keeping me in your thoughts and prayers. Finally, I am deeply grateful to God for granting me the health, time, ability and wisdom to make use of this wonderful opportunity.

Marthinus Jacobus Bekker, January 2016.

Table of Contents

Table of Figures

Table of Tables

Chapter 1 - Navigating the Sea of Asset Information

The purpose of this chapter is to introduce the research topic, describe the relevance and importance of the research topic, define the research problems, questions and approach, as well as provide the outline of the thesis.

1.1 Importance of Infrastructure Assets

Governments around the world face ***an acute need for new or modernised infrastructure*** that are essential for society to function and an economy to operate *(World Economic Forum, 2014).* These infrastructure assets include transport (e.g. roads, ports, rail, and airports), energy (electricity, oil and gas), water and sanitation, education and health care *(Male, 2010; NEPAD, 2012; National Treasury, 2013).* There is a global reliance on infrastructure assets and investment to achieve economic and social objectives *(Urban Land Institute, 2011).* These objectives include economic growth, global competitiveness, improving the quality of life for citizens and alleviating poverty *(World Economic Forum, 2014).* The worldwide stock of existing infrastructure is estimated to be worth US$ 50 trillion *(Political Economy Research Institute, 2009).* This is the same order of magnitude as the global stock market capitalisation and comparable to the global gross domestic product (GDP) of US$ 72 trillion *(World Federation of Exchanges, 2013; World Economic Forum, 2014).* A 1% increase in global infrastructure could boost the global GDP in the long term by between 0.05% and 0.25% *(Romp & de Haan, 2005).*

It was predicted in 2011 that the ***infrastructure investment*** to meet global demands over the next 25 years would reach US$ 50 trillion *(Urban Land Institute, 2011).* In 2013, the global infrastructure demand is estimated to be approximately US$ 3.7 trillion in annual expenditure *(World Economic Forum, 2013).* The infrastructure investment and demand for investment are applicable to both developed and developing countries *(Urban Land Institute, 2011; World Economic Forum, 2014).* Examples of infrastructure investment plans are: 1) the United Kingdom with a 5 year US$ 326 billion infrastructure investment plan; 2) Canada investing US$ 16 billion to address aging urban infrastructure; 3) Brazil launching a US$ 900 billion infrastructure plan; 4) India who is doubling its infrastructure investment to US$ 1 trillion; and 5) China investing more than US$ 1 trillion over 5 years in transport infrastructure *(Urban Land Institute, 2011).*

Merril Lynch reported that annual investment in new infrastructure in the ***emerging economies*** will be US$ 2.25 trillion, or 5% of GDP, over the next 3 years in order to obtain the same quality of life as in developed countries *(Edwards, 2010).* In the ***African continental context***, the African Union, via its New Partnership for Africa's Development agency, established the Program for Infrastructure Development in Africa (PIDA) *(NEPAD, 2012).* The goals of PIDA are: 1) to promote socio-economic development and poverty reduction in Africa through improved access to integrated continental infrastructure networks and services; and 2) to accelerate the delivery of current and future continental infrastructure projects *(NEPAD, 2012).* The current infrastructure deficit is hampering the African competitiveness in the world market, and its GDP growth, by an estimated 2% every year *(NEPAD, 2012).* Bridging the gap in infrastructure is thus vital for economic advancement and sustainable development on the continent *(NEPAD, 2012).* In the ***South African context***, the South African Government adopted a National Infrastructure Plan (NIP) *(Presidential Infrastructure Coordinating Commission, 2012).* The NIP supports the over-arching South African National Development Plan, with the aim of: 1) eliminating poverty and reducing inequality in South Africa by 2030; and 2) the integration of African economies *(National Planning Commission, 2011).* The value of major infrastructure projects in progress, or under consideration, in the South African public sector totals ZAR 4 trillion *(National Treasury, 2013).* The infrastructure investment includes the water sector. Seven new dams are being built and ZAR 42 billion has been made available to municipalities over the medium term, in order to improve reticulation, sanitation and sewerage processing plants *(National Treasury, 2013).* Both PIDA and the South African NIP support the United Nation's Millennium Development Goals *(United Nations, 2008).*

Infrastructure assets are essential for continued social, economic and environmental development and prosperity, whether such assets are owned by the state, privatised or a hybrid *(Male, 2010).* Some public infrastructure assets are classified as critical national installations *(The Water Environment Federation, 2007; Male, 2010).* These infrastructure assets include water, transport, education, health and energy *(Male, 2010).* The impact of critical infrastructure failures include potential social and welfare implications, damage to the economy, national security and loss of human life *(Rice & Almajali, 2014; Jaatun, Røstum, Peterson & Ugarelli, 2014).* Potable water, for example, is becoming a scarce commodity and sustainable water management has a direct impact on water scarcity and climate resilience *(World Economic Forum, 2014; World Bank, 2006).* Agriculture, mining and electricity generation are dependent on large-volume water supply *(National Treasury, 2013).* Access to

sufficient water is a constitutional right in South Africa. The Water Services Act No. 108 of 1997 recognises the right of access to basic water supply and sanitation, necessary to ensure sufficient drinking water and an environment that is not harmful to the health or well-being of citizens. Unsafe drinking water is one of the primary causes of the 1.5 million diarrhoea related deaths of children in developing countries each year *(World Health Organisation & United Nations Children's Fund, 2009).*

1.2 Importance of Infrastructure Asset Management

Organisations that rely heavily on ***infrastructure assets to function will face unprecedented challenges*** in the coming decades *(Male, 2010).* These include challenges posed by climate change, such as extreme weather (e.g. storms and flash floods in Europe) *(Male, 2010; Swiss-Re, 2009; Stern, 2007).* Physical assets operate in a dynamic environment where they are exposed to short, medium and long-term variability in ambient environmental conditions, including conditions caused by climate change *(Rayner, 2010).* The challenges of organisations and their infrastructure assets include the growing impact of sustainability issues (e.g. climate change), increased population placing a higher demand on services, constrained budgets, aging assets and workforce, security issues (e.g. terrorism), the pace of technological change and the scarcity of specialised resources *(Pilling, 2010; Edwards 2010).* The UK Institution of Civil Engineers concluded in 2009 that the UK's critical infrastructure is under more threat than ever before *(Edwards, 2010).* Organisations are under increasing pressure from customers, stakeholders, and regulators to provide better services without increasing cost or risk *(Pilling, 2010).* There is also increased pressure to regulate essential services in terms of social, economic and environmental sustainability *(Edwards, 2010).* On current projections, South Africa's water demand will exceed available supply between 2025 and 2030 *(National Treasury, 2013).*

The promising ***infrastructure investments are not moving forward*** as planned, and the supply of infrastructure cannot keep up with the demand *(World Economic Forum, 2014).* The global annual investment in infrastructure is US$ 2.7 trillion *(World Economic Forum, 2013*). There is a shortfall of US$ 1 trillion per year, which corresponds to 1.4% of global GDP *(World Economic Forum, 2013*). For example, the global road network expanded by 88% since 1990, but the global road traffic increased by 218% over the same period *(World Economic Forum, 2014).*

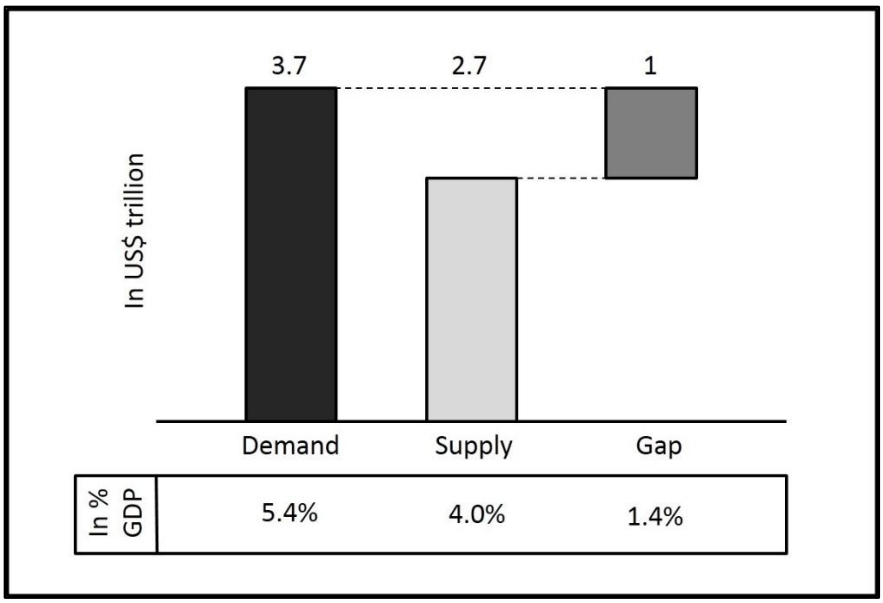


Figure 1-1 Global Investment Shortfall (World Economic Forum, 2014)

The American Society of Civil Engineers reported in 2009 that the infrastructure investment currently planned over the next 5 years for the USA is only 50% of the US$ 2.2 trillion investment required *(Edwards, 2010).* There is a widening divergence between the increased need for infrastructure investment globally, and the ability of governments to deliver the required infrastructure *(World Economic Forum, 2014).* With only 8% access to electricity in rural areas and 35% in urban areas, it is clear that infrastructure investment to expand energy access is a pressing issue for sustained development in Africa *(World Economic Forum, 2013).* The current infrastructure investment in the South African public sector is currently inadequate to realise a sustained impact on growth and household services *(National Treasury, 2013).* Notwithstanding the improvement in access to piped potable water inside dwellings, the infrastructure capacity and quality is still insufficient to adequately capture and distribute water to households and relevant industries *(Statistics South Africa, 2011; National Treasury, 2013).*

The ***maintenance and management of existing infrastructure*** is a concern in both developed and developing countries *(World Bank, 2006).* Aging infrastructure is the primary infrastructure maintenance related problem for developed countries *(World Economic Forum, 2014).* The majority of infrastructure assets in the European Union and North America were constructed during the 1950's to 1970's. These assets are now reaching the end of their expected useful life *(World Economic Forum, 2014).* For example: 1) the average age of the 607,380 bridges in the U.S. is 42 years and the average age of the 84,000 dams is 52 years; 2) a third of the rail bridges in Germany are over 100 years old; and 3) more than 20% of the 54,700 U.S. aging tap water systems supplying water to 49 million people are regularly in

violation of the U.S. Safe Drinking Water Act *(American Society of Civil Engineers, 2013; Kommission Zukunft der Verkehrsinfrastrukturfinanzierung, 2010; Duhigg, 2009).* The inability to keep the investment in maintenance in line with the investment in new infrastructure assets, is the primary maintenance related problem for developing countries *(World Economic Forum, 2014).* This is partially due to a political bias towards green-field infrastructure projects with higher visibility *(World Bank, 2006).* Approximately one third of the infrastructure needs in Africa, worth US$ 93 billion a year, is required for maintenance *(The International Bank for Reconstruction and Development & The World Bank, 2010).* The road network in China increased from 1.7 million kilometer (km) in 2001 to 4.1 million in 2011, and the maintenance requirement for this infrastructure will also increase in a similar quantum *(International Road Transport Union, 2009).* This problem is also applicable to the utilities sector. A large scale power outage in India left approximately 700 million people without electricity in 2012 *(Pidd, 2012).* According to the International Benchmarking Network for Water and Sanitation Utilities, the global percentage of non-revenue water vary from 4% to 65%, with a conservative estimated average of 30% *(World Bank, 2006).* Due to the lack of accurate and complete data from the developing world, the real average non-revenue water percentage for the developing world is estimated to be between 40% and 50% *(World Bank, 2006).* Approximately 45 million cubic meters of water are lost daily, primarily due to water leakage in the distribution networks and lack of maintenance *(World Bank, 2006).* This is enough to serve nearly 200 million people per day *(Word Bank, 2006).* The total cost of non-revenue water (NRW) is estimated to be US$ 14 billion per year, of which a third occurs in the developing word *(World Bank, 2006).*

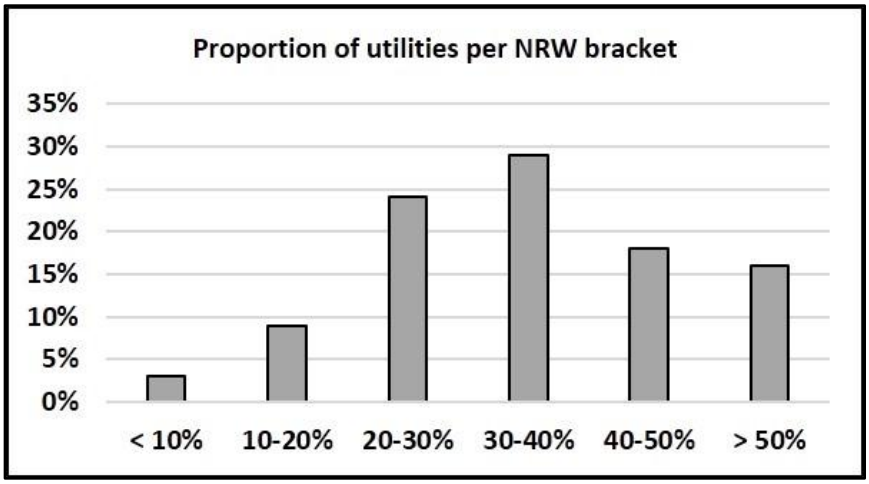


Figure 1-2 Non-Revenue Water Variation (Word Bank, 2006)

Reducing non-revenue water in the developing countries by only 50%, through improved maintenance of the existing infrastructure, could generate an extra US$ 2.9 billion per year for

water utilities *(World Bank, 2006).* The water saved in this manner could serve at least 90 million people without any extra investment or new water sources *(World Bank, 2006).* The South African Government developed the National Infrastructure Maintenance Strategy in 2006, and promulgated the Government Immovable Asset Management Act No. 19 of 2007 *(Department of Public Works, 2006).* The condition of infrastructure assets in South Africa improved since 2006, but municipal infrastructure is deteriorating in many places *(South African Institute of Civil Engineers, 2011)*. Bulk water facilities in small towns and rural areas, sanitation in many municipalities, as well as provincial and rural roads are areas of concern *(South African Institute of Civil Engineers, 2011).* Whilst 97% of South Africa's drinking water meets minimum quality standards, only 71% of wastewater is compliant, and the quality of the latter shows some degree of deterioration *(South African Institute of Civil Engineers, 2011).*

Effective control and governance of infrastructure assets by organisations are essential to realise value from these assets *(ISO, 2014).* Infrastructure asset management offers infrastructure asset dependent / intensive organisations and their external stakeholders with a rational set of principles for defining how corporate goals can be achieved and how the value of a business can be confirmed *(Lloyd, 2012).* This is achieved through managing risk and opportunity, in order to achieve the desired balance of cost, risk and performance *(ISO, 2014).* The benefits of infrastructure asset management include improved financial performance, managed risk, improved services and outputs, demonstrated social responsibility, demonstrated compliance, improved organisational sustainability, enhanced customer satisfaction, improved efficiency and effectiveness, improved health, safety and environmental performance, and informed asset investment decisions *(ISO, 2014; Institute of Asset Management, 2008).* There are numerous cases where asset management delivered short and long term benefits for both private and public sector entities *(Lloyd, 2012; Pilling, 2010).* Some of these are: 1) Manila Water of the Philippines reduced its non-revenue water from 63% in 1997 to 11% in 2010, through improved leak detection and maintenance*; 2)* UK Network Rail reduced their annual operating and maintenance cost by 8%, whilst punctuality of their service increased to above 90%; and 3) Scottish Power Generation experienced a reduction of 29% in operations and maintenance cost and a 22% improvement in plant availability *(Pilling, 2010; Lloyd, 2012; World Bank, 2006, World Economic Forum, 2014).*

1.3 Research Problem and Questions

Asset decision making is at the core of infrastructure asset management *(ISO, 2014).* Asset decisions include strategic decisions, such as capital investment, asset maintenance strategy, replacement versus refurbishment, shutdowns and outage strategy, as well as asset whole-life cost and value optimisation *(Global Forum on Maintenance and Asset Management, 2011).* Many decisions that matter, such as strategic infrastructure asset management decisions, are made by decision groups *(Zhang & Guo, 2014; Keen & Sol, 2008).* A variety of heterogeneous stakeholders and considerations must be balanced and trade-offs may therefore be required *(Zhang & Guo, 2014).* All phases of the asset life cycle, all asset management objectives and all relevant asset information should be considered when making asset related decisions *(Institute of Asset Management, 2008).* Examples of the dimensions to be considered are: 1) asset performance, maintenance history and condition; 2) asset value, life cycle costing and useful life; 3) asset risk, dependencies and criticality; 4) revenue generated from the asset, expected service levels, and demand management; and 5) social, political and environmental implications *(Institute of Asset Management, 2008; Lloyd, 2012; ISO 2014).* There is no universal standard formula, set of techniques or information base that is appropriate and suitable for all circumstances and for all organisations *(ISO, 2014; Lloyd, 2012).*

Evidence-based asset management decisions require meaningful, quality and timely ***asset information*** *(Institute of Asset Management, 2008).* Maintenance decision making is often hampered by substandard systems and information *(World Economic Forum, 2014).* Asset information from different sources must be fused, or harmonised, which may lead to conflicting evidence *(Zhang & Guo, 2014)*. It involves the integration of heterogeneous multi-source information to provide relevant, consistent, aggregated and meaningful evidence required to solve problems *(Fernández-de-Alba, Fuentes-Fernández & Pavón, 2013; Hammoudech & Newman, 2013).* An organisation's asset information is stored in a variety of digital systems *(Institute of Asset Management, 2008).* It originates from both the IT systems (e.g. ERP) and control systems (e.g. SCADA) *(ISO, 2014, Macaulay & Singer, 2012).* In addition, asset condition information is produced by a variety of asset condition technologies *(Lau & Dwight, 2011).* These categories of digital systems are typically found in an infrastructure asset intensive organisation, such as a water utility *(American Water Works Association, 2003).*

The environment of an asset intensive organisation is often ***extremely large, complex and heterogeneous in nature.*** This includes the digital technology landscape, asset information and the digital organisation.

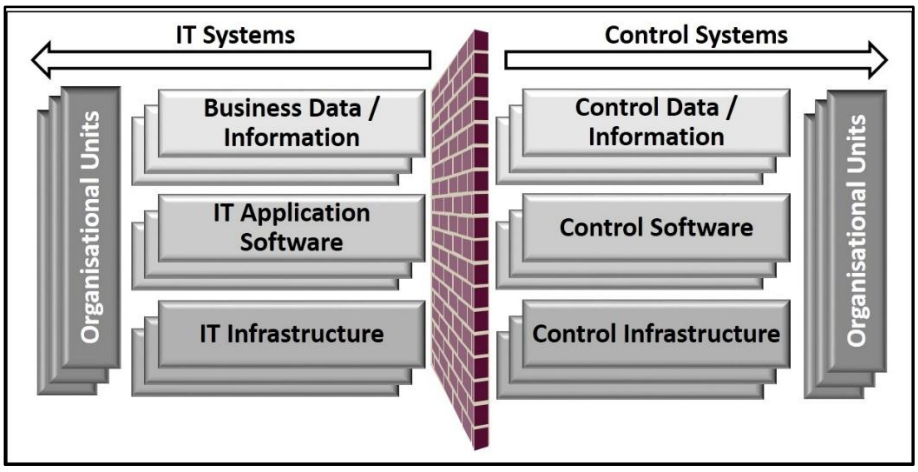


Figure 1-3 Complex and Heterogeneous Digital Environment

Digital systems storing asset information can be extremely large and complex *(ISO, 2014).* It can also consist of a variety of technologies *(Soloman, 2010; The Water Environment Federation, 2007).* This is primarily due to: 1) the convergence in digital technology; 2) the development of large scale distributed SCADA systems; and 3) the increasing adoption of sophisticated "smart" technology *(Rice & Almajali, 2014; Federal Energy Regulatory Commission, 2013; Global Water Intelligence, 2013).* There is an increased inherent risk to the infrastructure installations, or plants, if the IT and control system landscapes are integrated *(Macaulay & Singer, 2012).* This includes information security risks and the risk of disruption to the core operations of the organisation *(Anwar & Mahmood, 2014).* The asset information required for strategic asset decisions is characterised by two of the big data characteristics, namely volume and variety *(Chen & Zhang, 2014; Chang, Kauffman & Kwon, 2014).* The volume characteristic is caused by granular control system data (e.g. SCADA / telemetry data), as well as asset condition data created by asset condition assessment technologies *(von Petersdorff, 2013; Lau & Dwight, 2011).* The variety characteristic is caused by: 1) structured data (e.g. ERP, SCADA) and unstructured data (e.g. asset condition assessment technology); 2) electronic and paper-based media; and 3) data from both internal and external sources *(Chang, Kauffman & Kwon, 2014; ISO, 2014; Institute of Asset Management, 2008).* The IT and control system functions of a large and complex infrastructure asset intensive organisation are usually segregated *(The Water Environment Federation, 2007).* This could lead to: 1) a lack of knowledge sharing and collaboration; 2) unclear roles and responsibilities;

3) a lack of trust between the digital functions; and 4) resistance to change *(Campbell, 2011; Ahmad, Hadgkiss & Ruighaver, 2012; Kotter & Schlesinger, 2008).*

The ***governance*** maturity level within a control system environment is generally low, and operational process controls are not applied consistently between the IT and control system environments *(Pilling, 2010).* There is also the possibility of applying inappropriate compliance-based digital governance and operational process controls within the control system environment that do not adequately mitigate the associated risks of the digital landscape *(Port & Wilf, 2014; Verhoef, 2007).* There are many problems related to such a scenario in terms of: 1) collecting and transforming asset information into useful and reliable evidence to effectively support strategic infrastructure asset management decision making; and 2) implementing a sustainable change in the way of thinking, working, controlling and modelling, in relation to asset information management and digital governance.

The ***research questions*** to be addressed by this research are:

1. What is the content of a digital governance approach that addresses the information requirements of a modern infrastructure asset management philosophy and the associated problems?; and
2. What is the appropriate approach to implement enterprise-wide digital governance in a sustainable manner for a large, complex, heterogeneous asset intensive organisation?

1.4 Research Approach

This research uses design science as a research philosophy, adopting a pragmatic epistemological stance. The design science research philosophy is effectuated with the inductive-hypothetic research strategy, in order to achieve both scientific and practical contributions. Case studies, literature reviews and expert panel interviews are the primary research instruments to be used.

Design science is a ***research philosophy*** in which innovative artefacts are created to serve human problems, versus natural science explaining "how and why things are". It aims to solve real-world problems through the creation of artefacts, and in doing so, makes scientific contributions. These artefacts include constructs, models, methods, instantiations or combinations of the aforementioned. The science in design science for information systems research lies in the notion that knowledge and understanding of a design problem and its solution, are acquired in the building and application of an artefact *(March & Smith, 1995;*

Hevner & Chatterjee, 2010). Knowledge and understanding is acquired during this research by building, implementing and evaluating a digital governance approach that addresses the information requirements of infrastructure asset management and the associated problems in a large, complex, heterogeneous asset intensive organisation. There are three epistemological streams available to design science researchers, namely positivism, interpretivism and pragmatism. Pragmatism proposes that science is essentially a practical activity aimed at producing useful knowledge, rather than understanding the true nature of the world. Truth is essentially "what works in practice". The only sensible yardstick by which to judge a piece of knowledge is whether it is useful for a given interest *(Gonzalez & Sol, 2012; March & Smith. 1995; Mingers, 2004; Rorty, 1999).* Pragmatism is the appropriate epistemological stance for this research, because the research will focus on "what works" in terms of a digital governance approach in a large, complex, and heterogeneous infrastructure asset intensive organisation, in order to serve the interest of effective infrastructure asset management.

There are two primary ***research strategies,*** namely deductive and inductive. An inductive research strategy seeks to define a theory based on observations from given situations *(Trochim, 2006).* This research uses the inductive-hypothetic research strategy to effectuate the design science research philosophy, starting from a set of observations from which patterns are extracted (inductive reasoning) to formulate tentative hypothesis (designs) that are generalised and tested *(Gonzalez & Sol, 2012).*

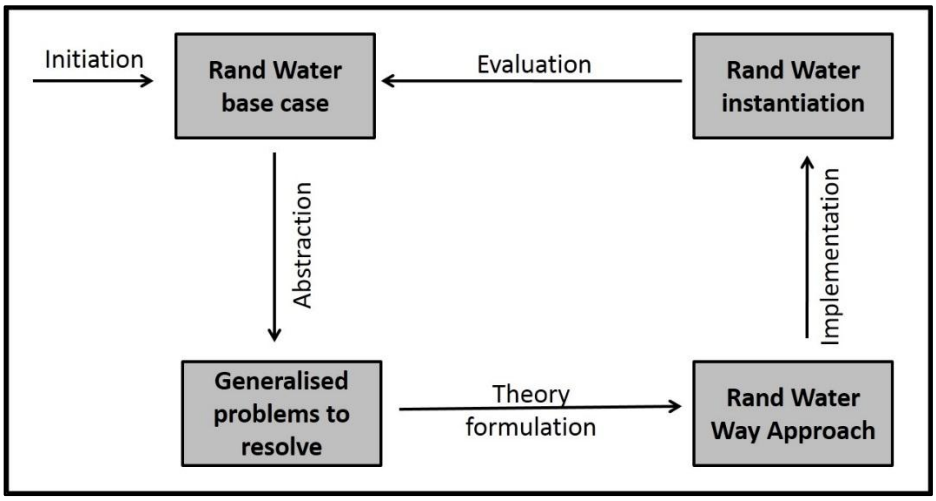


Figure 1-4 Research Strategy (Adapted from Sol, 1982)

The reason for employing the inductive-hypothetic research strategy of Sol *(1982)* is to ensure that the digital governance approach is shaped by the organisational context, thereby combining practice and theory. The researcher will be a reflective practitioner reflecting on the work

performed at the base case, as well as the digital governance approach designed for, and instantiated at, the base case. The ***inductive hypothetic research strategy*** is adapted and applied for this research as follows:

Phase	Description
Initiation	Literature-based research will be performed regarding the concepts and disciplines related to the research topic. The base case will be described. The description will include the minimum relevant characteristics of the base case. A large and well established regional water utility, namely Rand Water, will be the base case for this research. The outcome of this phase will be an in-depth understanding of the research topic and the base case. It will provide the lens, foundation and context for the rest of the research.
Abstraction	The related problems, issues or challenges will be abstracted from the base case, Rand Water. This includes technology, process and people related problems. The base case problems will be reflected upon and literature-based research will be performed, in order to improve the understanding of the problems related to the research topic and to generalise the problems. The requirements of the artefact, or theory, will be compiled based on the generalised problems to be resolved by the artefact.
Theory formulation	The generalised approach, called the Rand Water Way, will be designed. The design will include all the constituent parts required to establish the new way of asset information management and digital governance in support of infrastructure asset management. The four principles of design theory will be addressed by the design, namely the way of thinking, the way or working, the way of controlling and the way of modelling *(Seligmann, Wijers & Sol, 1989; de Vreede & Briggs, 2005).* Literature-based research will be performed, in order to design a proposed generalised approach that will resolve the problems identified when contextualised and implemented for an organisation.
Implementation	The generalised Rand Water Way will be instantiated at the base case, Rand Water, to resolve the problems abstracted from the base case. The instantiated description will include the contextualisation and detailed design of the generalised approach for the Rand Water environment. The instantiation will demonstrate the usage of the Rand Water Way at the base case.
Evaluation	The Rand Water Way will be tested in terms of usage, as well as perceived usefulness and usability *(Keen & Sol, 2008; Davis, 1989).* The usage, usefulness and usability of the Rand Water Way will be tested based on the Rand Water instantiation. The potential perceived usefulness and usability of the Rand Water Way will be tested at a selection of organisations similar to Rand Water. The aim of the test will be to determine if the implementation of a contextualised version of the Rand Water Way at these organisations, could potentially resolve their problems related to the research topic. The results will demonstrate the contribution of the Rand Water Way to the fields of information management and digital governance in support of infrastructure asset management in large, complex and heterogeneous infrastructure asset intensive organisations.

Table 1-1 Research Phases

Research instruments are specific methods that are used to execute a particular research strategy *(Gonzalez, 2010).* A case study involves the examination of a phenomenon in a natural setting or within its real-life context *(Darke, Shanks & Broadbent, 1998; Yin, 2003).* Multiple case studies were used during this research. This includes a base case for the abstraction of related problems, the instantiation of the Rand Water Way and the evaluation of the Rand Water Way. Case studies were also used to evaluate the potential utility of the Rand Water Way for similar organisations. This instrument was selected because of its suitability for understanding digital governance and information management related real-world problems in the context of the organisation. An interview is a data collection method where a researcher asks a respondent a set of questions and records the answers *(Neuman, 2003).* Interviews were performed during the evaluation phase to obtain the opinion of a panel of experts regarding the perceived usefulness and usability of the Rand Water Way. A questionnaire is a set of open and/or close ended questions administered to a number of respondents to gather information *(Neuman, 2003).* It can be qualitative, quantitative or mixed questionnaires *(Johnson & Turner, 2003).* A mixed questionnaire was used as an instrument to record the data gathered during the expert panel interviews. A literature review is the analysing of existing documentation on a given topic *(Neuman, 2003).* It was used during this research to improve the understanding of related concepts and disciplines, generalise the problems abstracted from the base case, and to substantiate the design of the Rand Water Way. The instruments will be used as follows per research phase:

Research Phase	Instruments	Application
Initiation	Case study Literature review	Defining the base case. Performing literature reviews regarding related concepts.
Abstraction	Case study Literature review	Abstracting the relevant problems from the base case. Performing literature reviews to generalise the problems and to compile the requirements of the artefact.
Theory formulation	Literature review	Performing literature reviews to design the artefact, namely a generalised approach that can be contextualised and applied at the base case and other similar organisations.
Implementation	Case study	Instantiating a contextualised version of the generalised approach at the base case, Rand Water.
Evaluation	Case study Expert panel interviews Questionnaires	Performing interviews with an expert panel from the base case and similar organisations, in order to evaluate the generalised approach. Using mixed questionnaires to record the data gathered during the expert panel interviews.

Table 1-2 Research Instruments

1.5 Thesis Outline

The thesis will include the following:

Chapter 1 – Navigating the Sea of Asset Information: The purpose of this chapter is to: 1) introduce the research topic; 2) describe the relevance and importance of the research topic; 3) define the research problem, questions and approach; and 4) provide the outline of the thesis.

Chapter 2 – Research Lens and Foundation: The purpose of this chapter is to provide the lens and foundation of the research, by defining the underlying associated concepts, disciplines and definitions from literature. It includes disciplines such as asset management, information technology and control systems, digital convergence, information management, enterprise architecture, as well as transition and change management.

Chapter 3 – Rand Water as Base Case: The purpose of this chapter is to present the base case for the research, namely Rand Water, by providing an overview of the minimum relevant characteristics of Rand Water. The base case description provides the context for the rest of the research, especially the instantiation. It will include a description of the Rand Water organisation, infrastructure assets, asset management practices and digital technology landscape.

Chapter 4 – Compilation of the Requirements: The purpose of this chapter is to compile the requirements of the artefact by identifying and describing the problems that must be resolved by the artefact. This will be achieved by abstracting the relevant problems from the base case and supplementing it from literature, in order to generalise the problems. The generalised problems will be identified and described in terms of technology, process and people related dimensions. The emphasis will be placed on those problems that impact information management and digital governance in support of infrastructure asset management.

Chapter 5 – Design of the Rand Water Way: The purpose of this chapter is to describe the artefact, namely a generalised integrated digital governance approach called "The Rand Water Way". The description of the Rand Water Way includes the overall philosophy, the underlying principles and the constituent parts of the approach. The chapter includes support for the characteristics of the approach through literature-based research.

Chapter 6 – Instantiation of the Rand Water Way: The purpose of this chapter is to describe the instantiation of the Rand Water Way. It includes a description of the contextualisation of the generalised Rand Water Way based on the characteristic of Rand Water, in order to resolve

the related problems at Rand Water. The description is structured according to the constituent parts of the Rand Water Way, namely strategy, architecture, information management, governance and transition management.

Chapter 7 – Evaluation of the Rand Water Way: The purpose of this chapter is to demonstrate the contribution of the Rand Water Way to the fields of information management and digital governance, in support of effective infrastructure asset management. This will be achieved by evaluating the Rand Water Way, in terms of its: 1) usage, perceived usefulness and perceived usability, as instantiated at Rand Water; and 2) potential perceived usefulness and potential perceived usability at similar organisations.

Chapter 8 – Epilogue: The purpose of this chapter is to present the closing remarks and a reflection on the research. This includes reflecting on the problem relevance, the research rigour, the evaluation of the artefact, the increase in knowledge, and the contribution made by the research. It will further provide direction regarding further related research opportunities.

Chapter 2 - Research Lens and Foundation

The purpose of this chapter is to provide the lens and foundation of the research by defining the underlying associated concepts, disciplines and definitions from literature. It includes concepts and disciplines, such as asset management, information technology and control systems, digital technology convergence, information management, enterprise architecture, as well as transition and change management.

2.1. Asset Management

An ***asset*** is an item, thing or entity that has potential or actual value to an organisation and its stakeholders *(ISO, 2014)*. For the purpose of this research, the term "asset" will refer to physical infrastructure assets. Physical assets usually refer to equipment, infrastructure, inventory and properties *(ISO, 2014)*. ***Asset management*** is a coordinated activity of an organisation to realise value from its assets by translating the organisation's objectives into asset-related decisions, plans and activities, using a risk based approach *(ISO, 2014)*. It is a collection of systematic and coordinated activities and practices through which an organisation optimally and sustainably manages its assets and asset systems, for the purpose of achieving the organisation's strategic plan *(Institute of Asset Management, 2008).*

The effective ***implementation of asset management*** requires a disciplined approach that includes: 1) determining appropriate assets to acquire or create; 2) how best to operate and maintain them; and 3) the adoption of optimal renewal, decommissioning and/or disposal options (*Institute of Asset Management, 2008).* There have been developments in the infrastructure asset management field during the last two decades to improve and formalise the infrastructure asset management discipline, such as the International Infrastructure Asset Management Manuals of 2000, 2002, 2006 and 2011, the Publically Available Specification on asset management (PAS 55) of 2004 and 2008, the Asset Management Landscape of 2011 and 2014, and the ISO 50001/2/3 series of standards on asset management of 2014 *(Institute of Public Works Australia, 2011; Institute of Asset Management, 2008; Global Forum on Maintenance and Asset Management, 2011; ISO, 2014).*

An ***asset management system,*** as defined by ISO 55001, is a management system for asset management, whose function is to establish the asset management policy and asset management objectives. It provides a structured approach for the development, coordination

and control of activities undertaken on assets by the organisation over different life cycle stages, and for aligning these activities with its organisational objectives *(ISO, 2014).*

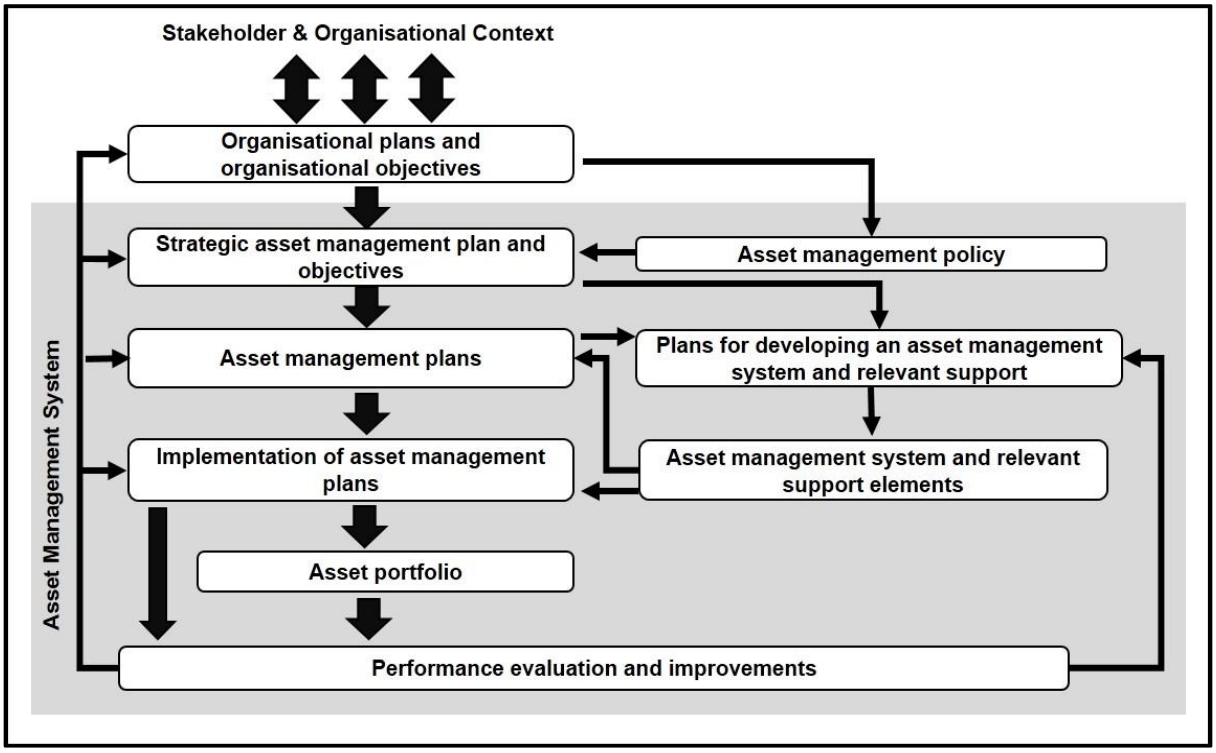


Figure 2-1 Asset Management System (ISO, 2014)

An asset management system consists of an asset management policy, strategic asset management plan (SAMP), asset management objectives and asset management plans. A strategic asset management plan, or asset management strategy, specifies: 1) how the organisational objectives are to be converted into asset management objectives; 2) the approach for developing asset management plans; and 3) the role of the asset management system in supporting the achievement of the asset management objectives. An asset management policy sets out the principles by which the organisation intends to apply asset management. Asset management plans are derived from the SAMP. These plans specify the activities, resources and timescales required for an individual asset, or a group of assets, to achieve the organisation's asset management objectives *(ISO, 2014).*

The organisation should ***evaluate the performance of its assets and its asset management system*** and improve these based on the result of the evaluation *(ISO, 2014; Burns, 2010).* An asset management system can help to gain an understanding of assets, their performance, the risk associated with assets, asset investment needs, and asset value as input to decision making. This includes asset management objectives, which may be quantitative or qualitative measurements *(ISO, 2014).*

The ***asset management objectives*** to be considered when making asset management decisions include the following:

Category	Objectives / Factors
For asset management	Net present value, return on capital employed, performance against plan, customer satisfaction scores, level of service, environmental impact, as well as society or reputational survey results.
For asset portfolios	Whole life cost of assets, return on investment (return on assets, return on capital employed).
For asset systems	Asset system reliability and performance (e.g. uptime, efficiency), as well as unit cost of products or services.
For individual assets	Reliability (mean time / distance between failures), asset condition, performance and health score, asset life cycle costs, and asset life expectancy.

Table 2-1 Asset Management Objectives (ISO, 2014; Institute of Asset Management, 2011)

Asset condition assessment is a key aspect of infrastructure asset management and asset decision making *(Lau & Dwight, 2011).* This includes the assessment of the condition of infrastructure assets underneath the earth's surface that provide essential utility services, such as complex networks of pipes and cables *(Costella, Chapman, Rogers & Metje, 2007).* It is critical to locate and assess the condition of these buried infrastructure assets, due to the ageing of the infrastructure and the increase in service demand *(Costella, Chapman, Rogers & Metje, 2007).* Asset condition assessment assists in identifying potential failure symptoms and remedial actions prior to any operational failure *(Lau & Dwight, 2011).* The asset condition assessment result is a key consideration when deciding whether an infrastructure asset should be repaired, refurbished or replaced *(Lau & Dwight, 2011).*

2.2. Decision Making

Decisions are the choices that shape the organisation's future. The effectiveness of decision-making is more closely related to the effectiveness of the organisation than any other factor *(Keen & Sol, 2008).* Asset management is the art and science of making the right decisions and optimising the delivery of value *(Institute of Asset Management, 2008).* Understanding how asset related decisions are made is therefore an important part of asset management *(ISO, 2014).*

"Quasirationality" is the combination of pure intuitive and pure analytical thought *(Dhami & Thomson, 2012).* It is increasingly widespread and beneficial in management decision making, depending on the situation and the type of decisions *(Dhami & Thomson, 2012).* Humans, with

all their strengths and flaws, make decisions that matter *(Keen & Sol, 2008).* Their skills, values, judgment and experience shape the decisions *(Keen & Sol, 2008).* When making decisions, managers seldom have all the relevant and necessary information or the time to apply pure analytical decision making *(Dhami & Thomson, 2012).* The quasirationality decision making method is beneficial when it is not cost effective or possible to compile a comprehensive and high quality collection of all the information necessary to apply a pure analytical decision making method *(Dhami & Thomson, 2012).* This information includes all possible futures, scenarios and alternatives, as well as the cost, risks and benefits associated with each option *(Dhami & Thomson, 2012).* It is also beneficial when there is a large degree of complexity or uncertainty over a long planning horison *(Dhami & Thomson, 2012).* Two examples of such a situation are long term asset management decisions and long term water resource system planning *(Matrosov, Woods & Harou, 2013).* Stakeholders are likely to make judgements about the organisation's assets and asset management practices based on their perceptions and views (*Matrosov, Woods & Harou, 2013).* These views need to be recorded and taken into account during the decision making process. However, the organisation also needs the capability to make evidence-based decisions *(Matrosov, Woods & Harou, 2013; ISO, 2014).* It should use a methodology that evaluates options of investing in new or existing assets and should consider aspects such as life cycle cost *(ISO, 2014).*

Collaboration and multi-stakeholder group decision making are key when trying to address complexity *(Zhang & Guo, 2014).* The increasing complexity of the socio-economic environment makes it less and less possible for a single decision maker to consider all relevant aspects of a decision making problem *(Zhang & Guo, 2014).* No one actor has all the information or skills to make effective choices *(Keen & Sol, 2008).* Decision processes increasingly require coordination across functions, geography, stakeholders and partners *(Keen & Sol, 2008).* Many decisions are made by decision groups consisting of heterogeneous stakeholders with different cultures, education, backgrounds, preferences, decision-making styles and knowledge *(Zhang & Guo, 2014).* Such groups can use a number of decision making rules, such as a consensus, majority, veto-by-one-vote or a compromise rule *(Zhang & Guo, 2014; Leung, Ji & Ma, 2013).*

Evidence-based decision making requires information from different sources. This can produce conflicting evidence, which can be resolved through information fusion *(Zhang & Guo, 2014).* It involves the integration of heterogeneous multi-source information to provide relevant, consistent, aggregated and meaningful evidence required to solve problems *(Leung,*

Ji & Ma, 2013; Fernández-de-Alba, Fuentes-Fernández & Pavón, 2013; Hammoudech & Newman, 2013). Speed and flexibility of evidence-based decision making is increasingly essential to respond to the pace of never-ending change, and the growing volatility and uncertainty of the competitive, political, social and economic environments *(Keen & Sol, 2008; Kotter, 2012).* Decision Enhancements Services (DES) aim to make a contribution to increasing decision process agility of organisations, which addresses speed, flexibility, coordination, collaboration and innovation *(Keen & Sol, 2008).* It is a fusion of the people that make the decisions, the process that influences the likelihood of making effective decisions, and the technology that provides multiple types and levels of support for both the people and processes *(Keen & Sol, 2008).*

The ***asset management decision-making criteria*** are influenced by the needs of internal and external stakeholders, the asset management policy and the risk attitude of the organisation. The decision-making criteria should be appropriate for the importance and complexity of the decisions being made and should support quantitative, semi-quantitative or qualitative decisions *(ISO, 2014).* The following are examples of asset management related decisions to be made during the life of an asset:

Asset Decisions	Description
Aging assets strategy	Decide on the appropriate interventions for assets approaching the end of their economic life, by considering life extension options, future needs for the asset, cost of disposal, and the cost and risk of alternative interventions.
Capital investment	Decide on the capital expenditure requirements necessary to deliver the strategic plan, by considering whole-life cycle cost and benefits.
Operations and maintenance	Decide on the appropriate maintenance requirements, by considering various maintenance and inspection activities to mitigate the risk.
Resourcing strategy and optimisation	Decide on the optimal use of people, plant tools and materials to deliver the required asset management activities, by considering risk, work priorities and spares inventory.
Shutdowns and outage strategy optimisation	Decide on the optimal strategy for shutdown and outages, by considering the cost of the outage, the risk associated with work being undertaken, and the efficiencies gained through the use of longer shutdowns and outages.
Whole-life cost and value optimisation	Decide on the different renewal and maintenance interventions via trade-offs between the cost and benefit of different interventions.

Table 2-2 Asset Decisions (Global Forum on Maintenance and Asset Management, 2011)

Asset related decisions consist of: 1) operational decisions made by an operator or a control system based on real-time data supplied by instrumentation; 2) tactical decisions made on a

daily to monthly basis by supervisors or management, such as shutdowns and daily maintenance schedules; and 3) strategic decisions, such as new asset investment, and asset replacement versus refurbishment decisions *(Rasmussen & Goodstein, 1987).* This research will focus on the strategic level asset decisions.

2.3. Information Management

Information Management is the activities and the organisation structure required to control an enterprise's electronic and physical information assets in a way that optimises access by all who have a share in that information, or a right to that information *(Association of Information and Imaging Management, 2014).* The overall purpose of information management is to ensure the integrity and availability of information in a timely manner *(Liell-Cock, Graham & Hill, 2009).* Information, which is interpreted data, is an intangible asset and strategic resource that is important to an enterprise's business *(von Solms & von Solms, 2006; Iyamu, 2011; Uçaktüçrk & Villard, 2013; Kooper, Maes & Lindgreen, 2011).* It is any communication or representation of facts, data, or opinions *(The Open Group, 2009).* Information can exist in many media or forms, such as printed or written on paper, stored electronically, transmitted by post or electronically, shown on films (e.g. audio-visual), numerical, graphical, textual, or spoken in conversations *(The Open Group, 2009).* Information can also be structured or unstructured as well as formal or informal *(IT Governance Institute, 2012).* During the information cycle, business processes generate and process data, transforming it into information and knowledge and ultimately generating value for the organisation *(IT Governance Institute, 2012).*

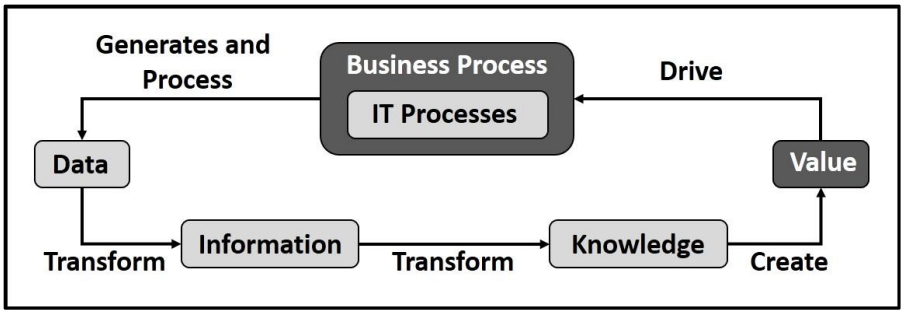


Figure 2-2 Information Life Cycle (IT Governance Institute, 2012)

Information has many definitions and should always be ***viewed within its context*** *(Kooper, Maes & Lindgreen, 2011).* Information and the discipline of information management are defined in, and viewed from, the context of the field of application, such as library and information science, information systems, records management or knowledge management *(Madsen, 2013).* For the purpose of this research, information management is rooted in the

discipline of information systems. Information management consists of a number of key overlapping and complementary concepts and activities, such as information architecture and standards, information security and protection, data quality management, meta data and master data management, business intelligence or data analytics, systems integration, data transfer and movement, protection of personal information and privacy, compliance management, data ownership or stewardship, information risk management, information categorisation and classification, data definition language or taxonomy, as well as document and image management *(Association of Information and Imaging Management, 2014; Liell-Cock, Graham & Hill, 2009; van Niekerk & Maharaj, 2011; Chang, Kauffman & Kwon 2014; Chen & Zhang, 2014; Kwon, Lee & Shin, 2014; Iyamu, 2011; Jouine, Arfa & Aissa, 2014).*

Both the data consistency and data completeness dimensions of ***data quality*** are important for decision making *(Kwon, Lee & Shin, 2014).* Data consistency is about keeping data uniform as it moves across the network and is shared by various digital systems *(Kwon, Lee & Shin, 2014).* Data completeness refers to the degree to which all data, necessary for current and future business activities (e.g. decision making), are available in the organisation's data repository *(Kwon, Lee & Shin, 2014).*

Information security has become crucial for organisations to minimise risks that endanger organisations' operations, and to maintain the confidentiality, integrity and availability of information *(ISO, 2005; Silva, de Gusmão, Poleto, e Silva & Costa, 2014).* Availability relates to the timely and reliable access to information. The integrity of information relates to the assurance regarding the quality of the information. The confidentiality of information relates to privacy requirements and the protection required against the misuse of personal and proprietary information *(Anwar & Mahmood, 2014; Wang & Shuo, 2013).* The causes of the security risks include both intended and unintended threats from internal and external to the organisation *(Anwar & Mahmood, 2014; Campbell, 2011).* It also includes human, environmental and technological related threats *(Jouine, Rabai & Aissa, 2014).* Unintended threats include human error, software errors, equipment failures and natural disasters *(Campbell, 2011; Jouine, Rabai & Aissa, 2014).* Intended threats include cyber terrorisms, industrial espionage and disgruntled employees *(Campbell, 2011; Jouine, Rabai & Aissa, 2014).* Malicious software and unauthorised access are two of the primary attack methods of intended threats *(Anwar & Mahmood, 2014; Campbell, 2011).* Identity and access management, via a role-based access control model, is still the most important information security control *(Fuchs, Pernul & Sandhu, 2011).* The ultimate goal of information system

security is to protect the information system, enabling it to fulfil its organisational mission as a whole *(Zhiwei & Zhongyuan, 2012).*

The objective of ***information security risk management*** is to protect the most critical information assets from high-risk scenarios, as well as balancing the cost of control and the level of security provided *(Shedden, Ruighaver & Ahmad, 2010).* It is one of the most important parts of a security program in IT organisations *(Tohidi, 2011).* It allows the organisation to determine whether they are protecting their information assets using the most cost effective means *(Webb, Ahmad, Maynard & Shanks, 2014).* This is achieved by: 1) identifying security risks related to critical information assets; 2) prioritising them according to severity or security exposure; and 3) developing and implementing effective and economically viable controls to mitigate the risk *(Shamala, Ahmad & Yusoff, 2013; Webb, Ahmad, Maynard & Shanks, 2014).* Security exposure is represented as a function of the probability of the threats and the expected loss, due to the vulnerability of those threats *(Feng, Wang & Li, 2014).*

Information and information management are associated with a number of closely related and overlapping disciplines and concepts, such as information governance, records management, knowledge management and "big data". ***Information Governance*** involves establishing an environment and opportunities, rules and decision-making rights for the valuation, creation, collection, analysis, distribution, storage, use and control of information *(Kooper, Maes & Lindgreen, 2011).* It also answers the following questions: "what information do we need, how do we make use of it and who is responsible for it?" *(Kooper, Maes & Lindgreen, 2011).* Information governance specifies the accountability for the management of an organisation's information assets *(Association of Information and Imaging Management, 2014).* It is an umbrella function for legislative compliance and records management *(Sheperd, Stevenson & Flinn, 2010).* ***Records management***, also referred to as records information management, is the practice or discipline of controlling and governing what are considered to be the most important records of an organisation throughout the records life-cycle, from the time it is conceived to the time it is disposed of *(ISO, 2001).* Information records need to be identified, classified, prioritised, stored, archived, protected, made available, and disposed of when required *(Liell-Cock, Graham & Hill, 2009; ISO, 2001).* ***Knowledge management*** is an approach that aims to improve an organisation's capabilities through better use of the organisation's individual and collective knowledge resources *(European KM Forum, 2002).* Knowledge is information transformed into "understanding" *(European KM Forum, 2002).* Explicit knowledge is knowledge that has been documented, whilst tacit knowledge is personal

knowledge resident within the mind of an individual *(BSI, 2003).* ***Big data*** are data sets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyse *(Chang, Kauffman & Kwon, 2014).* However, big data is also characterised by velocity, variety and value *(Chen & Zhang, 2014; Chang, Kauffman & Kwon, 2014).* The term "velocity" indicates the speed of data and "variety" describes the range of data types and sources *(Chen & Zhang, 2014).* "Value" refers to information that is relevant, useful and valuable for a specific purpose *(Lehman & Heagy, 2014).* Big data comes from everywhere, in a large variety of formats and may flow in real-time streams for analysis and decision making *(Chang, Kauffman & Kwon, 2014).* This new trend in decision support is evocative of: 1) what happened in the 1990s with the emergence of data mining; and 2) the new emphasis on data with a large number of dimensions and much higher complexity (e.g. spatial, multimedia, XML and Internet data) *(Chang, Kauffman & Kwon, 2014).*

Information management is an ***enabler of asset management*** *(Institute of Asset Management, 2008).* It requires meaningful, quality and timely asset information *(Institute of Asset Management, 2008).* Asset decision making and information requirements are tightly dependent, and it is essential to sort out any underlying data issues *(Woodhouse, 2010).* All asset information must be controlled across the full information life cycle *(Institute of Asset Management, 2008).* An organisation should determine the information needs related to its assets, asset management and its asset management system *(ISO, 2014).* The following ***asset information dimensions*** should be considered, when an organisation identifies the appropriate information required for its asset decision making process:

Dimension	Examples of Information
Business process	Process performance indicators, asset related processes and procedures.
Contract management	Vendor information, third party agreements, warrantees.
Financial	Acquisition date, life cycle costing analysis, useful lives of assets, residual and replacement values.
Maintenance management	Work and maintenance schedules, historical asset failures, refurbishment or replacement dates, future maintenance requirements.
Performance	Asset performance data, continuous improvement objectives, regulatory reporting.
Risk management	Operational risk management, business continuity.
Service delivery and operations	Service levels, performance objectives, asset performance, future operational requirements.
Strategy and planning	Corporate service levels and objectives, asset strategy, and demand management.

Dimension	Examples of Information
Technical and physical asset properties	Ownership, unique identification, criticality, designs, design parameters, vendor information, physical location, condition, in service dates, asset dependencies.

Table 2-3 Asset Information Dimensions (ISO, 2014; Institute of Asset Management, 2008)

Considering these asset information dimension will ensure that all phases of the asset life cycle, all asset management objectives and all asset information from internal and external sources are considered *(Institute of Asset Management, 2008; ISO, 2014).* The external sources include key suppliers, regulators or other stakeholders *(ISO, 2014).* The documented asset information include asset registers, drawings, contracts, licenses, legal, regulatory and statutory documents, policies, standards, guidance notes, technical instructions, procedures, operating criteria, asset performance data and asset condition data *(Institute of Asset Management, 2008).*

When applying information management and governance to asset management, an ***asset information strategy*** is required *(Global Forum on Maintenance and Asset Management, 2011).* The purpose of this strategy is to ensure that the information and information management efforts are appropriate and feasible for the organisation *(ISO, 2014).* It defines the approach to the management and governance of the asset information, necessary to support the implementation of an organisation's asset management strategy *(Global Forum on Maintenance and Asset Management, 2011).* The asset information strategy further specifies the method of asset information definition / specification, collection, maintenance, reporting and disposal, whilst recognising the life cycle cost of the information in relation to its criticality for asset management decision making. *(Edwards, 2010).* The following should be considered when determining the asset information strategy in support of asset management decision-making:

Considerations	Description
Accountability and responsibilities	The determination, assignment and periodic review of accountability for stewardship of data, the responsibility and competencies required for collecting, interpreting, utilising and reporting information *(ISO. 2014).*
Data importance, value and prioritisation	The information should be of a quality appropriate for the asset management decisions and activities it supports (*Institute of Asset Management, 2008*). Data should be prioritised based on the value or criticality of the data, and the granularity of the data versus the cost and complexity of collecting, managing and sustaining the information *(ISO, 2014; Edwards, 2010).*

Considerations	Description
Processes and controls	The establishment and continuous improvement of controls, specifications and levels of accuracy for data, as well as data collection processes for data from external stakeholders *(ISO, 2014).*
Systems and data integration	The linkage, harmonisation and consolidation of financial and non-financial asset information from different information resources that is appropriate for the size, complexity and capability of the organisation *(ISO, 2014; Lloyd, 2012).*
Terminology	The alignment of information requirements to different levels and functions of the organisation, including the use of common terminology, in order to ensure consistent meaning and understanding of information *(ISO, 2014).*

Table 2-4 Asset Information Strategy Considerations

2.4. Digital Technology

Appropriate resources need to be in place for infrastructure asset management, such as funding, human resources and ***information technology support*** *(ISO, 2014).* The systems required for asset information should enable the organisation to identify, collect, retain, transform and disseminate asset management information. Asset management data is stored in a variety of systems and some asset data originates from control systems *(ISO, 2014; Institute of Asset Management, 2008).*

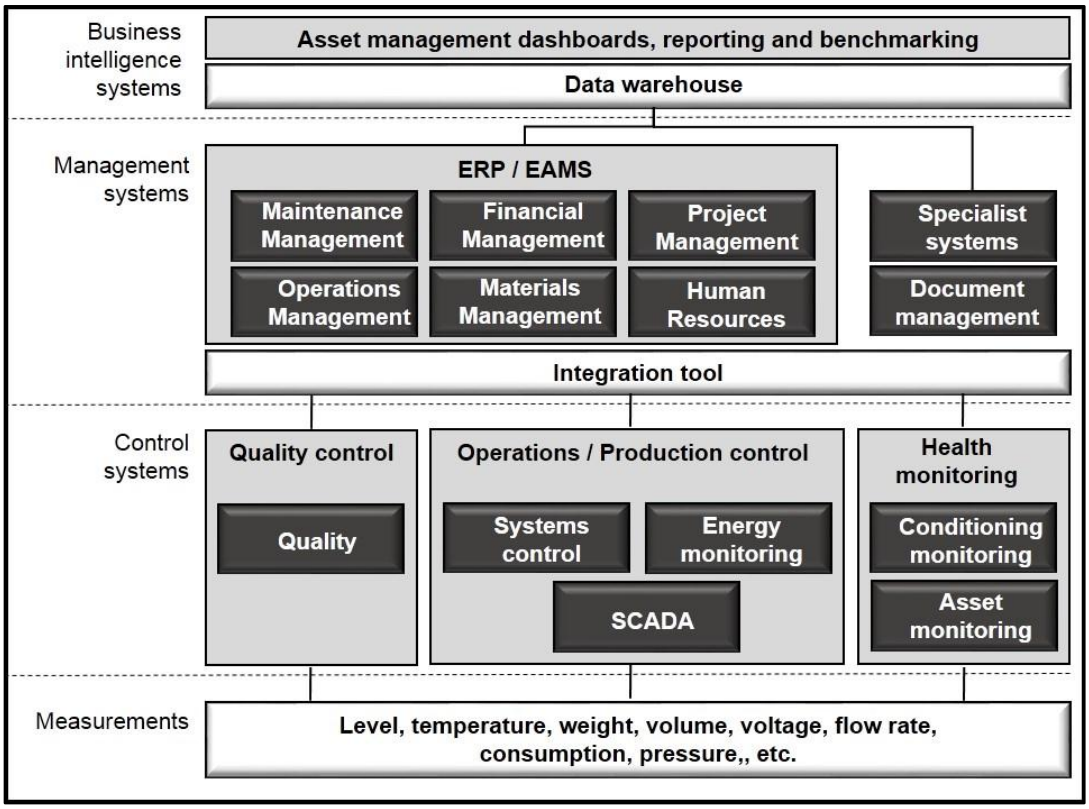


Figure 2-3 Asset Management Systems Landscape (Pragma & Aurecon, 2012)

The systems landscape required for infrastructure asset management includes: 1) business intelligence systems to support strategic asset management decisions; 2) management systems, such as an Enterprise Resource Planning (ERP) or an Enterprise Asset Management System (EAMS); 3) Control Systems and the related instrumentation for plant operations and control, health monitoring, and product quality control; and 4) integration tools to transfer asset data between systems *(Pragma & Aurecon, 2012).* IT systems focus on the management, movement and manipulation of data *(Macaulay & Singer, 2012).* Control systems focus on the management, movement, and manipulation of physical systems, such as valves, actuators, drives, and motors (Macaulay & Singer, 2012). For the purpose of this research, the term ***digital technology*** is used as a collective term for information technology (IT) and control systems, as required for infrastructure asset management.

Information Technology (IT) is the resources required to acquire, process, store and disseminate information *(ISO, 2008).* This term also includes Communication Technology (CT) and the composite term Information and Communication Technology (ICT) *(ISO, 2008).* Alternate terminology commonly adopted for IT over the years include data processing, computer systems, database systems, management systems and information systems *(The Water Environment Federation, 2007; The Open Group, 2009; Soloman, 2010; Institute of Asset Management, 2008; Pragma &* Aurecon*, 2012).* IT typically enables the supporting, or administrative-intensive, business processes of an infrastructure asset intensive organisation (e.g. financial management, human resources, maintenance management, project management and materials management) *(Institute of Asset Management, 2008; Pragma & Aurecon, 2012).* It includes the required hardware, software and firmware *(The Water Environment Federation, 2010; Soloman, 2010).*

Control systems are also referred to as operational control systems, automation, operational technology, process control systems, industrial control systems, telemetry systems, operational technology, and industrial systems *(The Water Environment Federation, 2007 & 2010; Kiameh, 2003; King & Knight, 2003; Soloman, 2010; Pragma & Aurecon, 2012**;** Macaulay & Singer, 2012; Gartner, 2013).* These systems are applied in various industries, including water and sanitation services, logistics (transport and postal), defence, energy, facilities management, mining, health care and manufacturing *(Kiameh, 2003; King & Knight, 2003; Soloman, 2010, Macaulay & Singer, 2012).* Process control is the regulation or manipulation of a process' conditions to bring about a desired change in its outputs *(Parker, 1984).* Instruments collect data about the state of a process or process devices, transmit the data to a database and notify

operators of unwelcome changes or conditions *(The Water Environment Federation, 2007).* Operators, or an automated control system, modify the process variables to bring it within an acceptable range based on the data and notifications received (e.g. alarms) and pre-defined process condition parameters *(The Water Environment Federation, 2007).* A process device, or final control element, is any device (e.g. pump, valve, motor, meter, and heater) that can change a process *(The Water Environment Federation, 2010).* There are three types of control systems, namely: 1) plant control systems that only control processes or plants; 2) data acquisition systems that only collect data from process devices or the environment; and 3) systems that fulfil both the two abovementioned purposes *(Macaulay & Singer, 2012).* Typical examples of control systems in the water sector are supervisory control and data acquisition systems (SCADA), automated meter reading (AMR) systems and laboratory information management systems (LIMS) *(Global Water Intelligence, 2013).* A SCADA system consists primarily of a human-machine interface (HMI) for operators, a data historian for storing longer term data, instrumentation and a communication or telemetry network to transmit messages between the other components of the system *(King & Knight, 2003).* Typical instruments that are used by process control systems include sensing equipment, digital recorders and data loggers, as well as controllers, such as programmable logical controllers (PLCs). Sensing equipment (e.g. sensors, meters, probes) measure variables in real-world phenomena, such as temperature, pressure, flow, chemical compositions, distance, speed, voltage, clearance margins, level, position, length and weight *(Fernández-de-Alba, Fuentes-Fernández & Pavón, 2013; Hammoudech & Newman, 2013).*

Asset condition technology is an additional category, or extension, of control system technology relevant to infrastructure asset management. A combination of technologies and techniques are used, since there is no single technology that can locate all underground utility services or assess the condition of the infrastructure assets with certainty *(Costella, Chapman, Rogers & Metje, 2007).* This includes electromagnetic and radio frequency line locators, ground penetrating radar, infrared thermography sonar and laser surveys, closed-circuit television, magnetic flux leak detection equipment, and ultra sound probes *(Costella, Chapman, Rogers & Metje, 2007; Lau & Dwight, 2011).*

The ***convergence in digital technology*** meant that microprocessor-based IT products now enable nearly all process control system elements *(The Water Environment Federation, 2007; Macaulay & Singer, 2012).* It reduced the cost of control systems, made it less proprietary and more flexible, improved the usability of operator interfaces, enabled integration with other

computerised systems, enabled advanced process control solutions (e.g. intelligent decision support systems or "smart" devices and networks) and improved productivity and efficiency *(The Water Environment Federation, 2007; Macaulay & Singer, 2012; Global Water Intelligence, 2013).* The IT products that contributed to the above include industrial grade Windows-based personal and handheld computers, the internet (e.g. "internet-of-things" and "industrial internet of things"), Ethernet-based networks (e.g. TCP/IP), graphical user interface, relational databases, off-the-shelve automation software products, artificial intelligence and fuzzy logic, mobility-related technology, graphical user interfaces and touch-screen technology. *(The Water Environment Federation, 2007; Global Water Intelligence, 2013; Soloman, 2010; Fernández-de-Alba, Fuentes-Fernández & Pavón, 2013; World Economic Forum, 2015).* A benefit of this convergence for infrastructure asset management is that the data collected and stored by control systems can be interfaced to and used by other digital systems for record retention, compliance, decision making, and further business processing purposes *(Fernández-de-Alba, Fuentes-Fernández & Pavón, 2013; Hammoudech & Newman, 2013).* The convergence in digital technology, especially wireless communications technology, also enabled the size and complexity of computerised control systems to increase, resulting in large scale distributed control systems *(Macaulay & Singer, 2012; Wang & Shuo, 2013).*

There has also been developments in ***computerised control system security*** since the International Society of Automation started working on security standards in 2002, for what it called "industrial automation and control systems" *(Macaulay & Singer, 2012).* These developments include "Mitigations for Vulnerabilities Found in Control System Networks" published by the Department of Homeland Security in 2006, NIST 800-82: "A Guide to Industrial Control System Security" published by the National Institute of Standards and Technologies, and NIST 800-53 revision 2 "Recommended Security Controls for Federal Information Security Standard", as well as industry-specific security standards and guidelines published by the North American Electricity Reliability Council and the Nuclear Regulatory Commission *(Macaulay & Singer, 2012).*

2.5. Enterprise Architecture

An ***architecture*** is a set of descriptive representations that are relevant for describing something intended to be created and constitutes the baseline for changing an instance of that "something" once it has been created *(Zachman, 2003).* It is the fundamental organisation of a system

embodied in its components, their relationships to each other and the environment, as well as the principles governing its design and evolution *(ISO, 2008).* An ***enterprise architecture*** is the set of descriptive representations relevant to describing an enterprise *(Zachman, 2003).* It is defined as the organising logic for an organisation's operating model, core business processes and IT capabilities that are captured in a set of principles, policies, and technical choices *(Ross, 2004; Fonstad & Robertson, 2004).*

The ***purpose of an enterprise architecture*** is to optimise the often fragmented legacy of manual and automated processes across the enterprise into an integrated environment that is responsive to change and supportive of the delivery of the business strategy *(Zachman, 2003; The Open Group, 2009).* It allows individual business units within the enterprise to innovate safely in their pursuit of competitive advantage, whilst ensuring that the needs of the enterprise for an integrated IT strategy are met *(The Open Group, 2009).* It is key to dealing with the complexity of an enterprise, as well as change within an enterprise, by enabling the impact of a change to be analysed and the different variants of the target architecture to be evaluated *(Zachman, 2003; Šaša & Krisper, 2011).* There are four primary uses for an enterprise architecture, namely: 1) presentation, collaboration and communication between stakeholders; 2) target state setting, change impact assessment, gap analysis and transition planning; 3) improving the knowledge and understanding of the organisation, the architecture domains and the relationship between the domains; and 4) ensuring coherency, alignment and consistency in different parts of a business system, including the technology and the data *(Šaša & Krisper, 2011; Kang, Lee, Choi & Kim, 2010).* Management needs to understand the overall architecture of its company's IT applications, what information resources are out there, and what condition they are in *(Nolan & McFarlan, 2005).*

An enterprise architecture includes: 1) the organisational structure and business processes; 2) the information, or data; and 3) the information technology services and infrastructure of the enterprise *(Šaša & Krisper, 2011; Kang, Lee, Choi & Kim, 2010).* A typical enterprise architecture consists of the three generic architectures (architecture domains), individual solution architectures, a vision (target) architecture, a migration plan to achieve the vision architecture, architecture principles, the architecture implementation governance approach and cross-layer architectures *(The Open Group, 2009).*

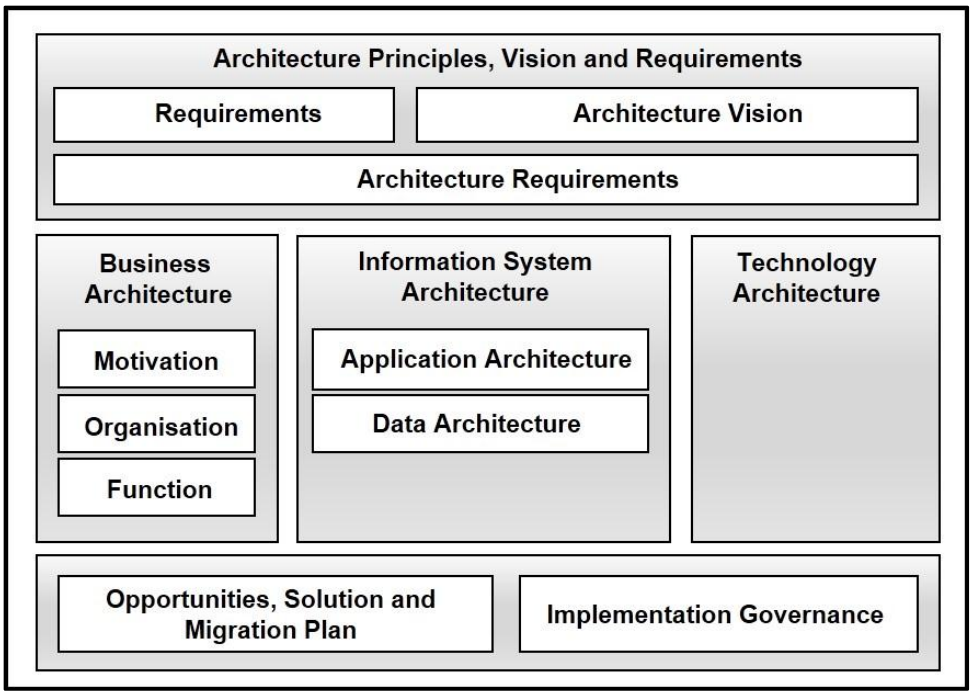


Figure 2-4 Architecture Content Framework (The Open Group, 2009)

The generic architectures, or architecture domains, are:

Architecture / Domain	Description
Business architecture	Also referred to as the business process domain or the business layer. It defines the business strategy, governance, organisation, and key business processes. Business architecture artefacts capture architectural models of the business operations, looking specifically at factors that motivate the enterprise, how the enterprise is organisationally structured, and what functional capabilities the enterprise has.
Information systems architecture	Also referred to as the Information Architecture. It consists of the data and applications architectures. • **Data architecture**: Describes the structure of an organisation's logical and physical data assets and resources. • **Application architecture**: Also referred to as the application layer. It provides a blueprint for the individual application systems, their interactions, and their relationship to the business processes of the organisation.
Technology architecture	Also referred to as the technology domain or technology layer. It describes the logical software and hardware capabilities that are required to support the deployment of business, data, and application services. This includes IT infrastructure, middleware, networks, communications and processing.

Table 2-5 Enterprise Architecture Domains (The Open Group, 2009; Šaša & Krisper, 2011)

A ***solution architecture*** is a description of a discrete and focused business operation and how IT supports that operation. It typically applies to a single project *(The Open Group, 2009).* An ***architecture vision,*** or target architecture, is the description of a desired future state of the

architecture being developed for an organisation *(Šaša & Krisper, 2011).* It might include a ***roadmap, or migration plan***, to show the evolution, or transition, of the architecture to the desired target state via a portfolio of prioritised projects and programs *(Giachetti, 2012; Agievich & Skripkin, 2014).* There are also ***cross-layer views, or sub-domains,*** that supplement and extend the generic enterprise architecture domains *(Mamaghani, Madani & Sharifi, 2012).* Examples of such cross-layer domains include an enterprise information security architecture and a performance architecture *(Shariati, Bahman & Shams, 2011; Pulkkinen, Naumenko & Luostarinen, 2007).*

Architecture governance is the practice by which enterprise architectures are managed and controlled at an enterprise-wide level *(The Open Group, 2009; ISACA, 2012; IT Governance Institute, 2012).* A set of defined standards is the measure most commonly used to govern enterprise architecture *(The Open Group, 2009).* All architectures, digital functions and digital projects must comply with these standards *(IT Governance Institute, 2012).* Standardisation is also a method to address complex problems *(Kluth, Jäger, Schatz & Baurenhansl, 2014).* Standards can include data standards (e.g. formats, origin, ownership, replication, and access restrictions), application standards (e.g. interoperation and communication, presentation and style) and technology standards (e.g. hardware and software products, network protocols) *(Ross, 2004).* The lack of interoperability, namely the ability to share information and services, is a key risk and therefore a key architectural governance requirement in a complex or extended enterprise *(Kang, Lee, Choi & Kim, 2010; Zandi & Tavana, 2012).*

There are a number of generic and domain-specific ***enterprise architecture frameworks***, meta-models, approaches, methods and modelling languages that were developed. These include the Zachman Framework for Enterprise Architecture, The Open Group Framework (TOGAF), Integration Definition Method (IDEF), Gartner Enterprise Architecture Method (GEAM), US Federal Enterprise Architecture Framework (FEAF), IEEE Computer Society standard (IEEE 1471-2000), ISO 42010, Business Process Modelling Language (BPML), Unified Modelling Language (UML), and the Archimate Modelling Language. It also includes frameworks focusing only on risk-driven enterprise information security architectures, such as SABSA and RISE *(Zachman, 1987; The Open Group, 2009; ISO, 2008; Kang, Lee, Choi & Kim, 2010; Šaša & Krisper, 2011; Zandi & Tavana, 2012).*

2.6. IT Governance

More and more companies are becoming ***dependent on computer systems*** for their daily operations, to grow the business, and to improve business performance *(Zhiwei & Zhongyuamn, 2012; Kerr & Murthy, 2013).* In 2012, 94% of organisations globally considered IT to be very important to the delivery of the overall business strategy and vision (*ISACA, 2012).* This situation has been fairly consistent with an increase from 91% in 2004 *(IT Governance Institute, 2011).*

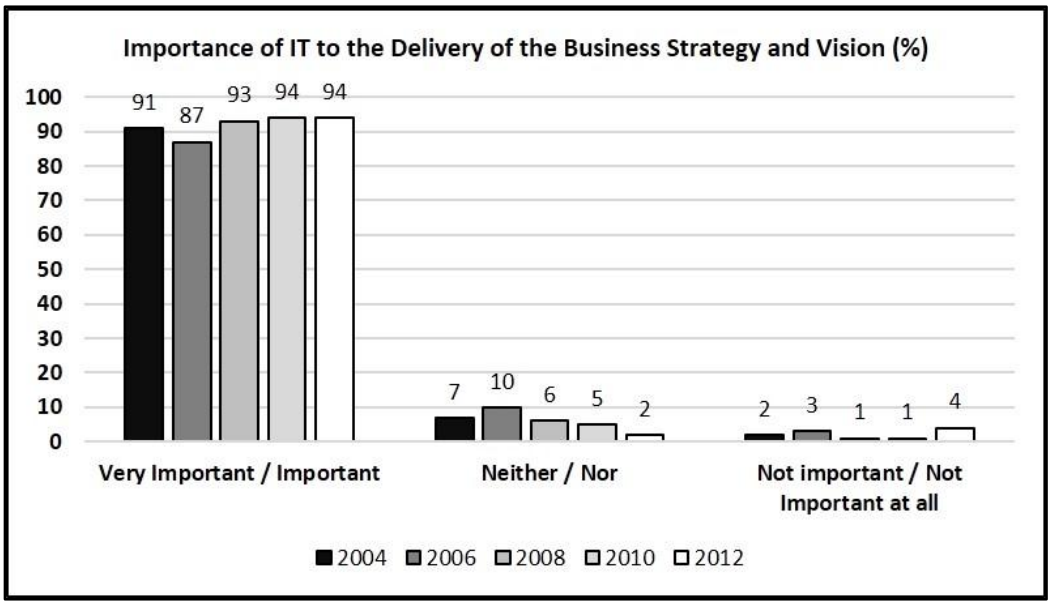


Figure 2-5 Importance of IT (IT Governance Institute, 2011; SACA, 2012)

These IT capabilities and the pervasiveness of IT bring about significant risks to the organisation, and the governance and control of IT has therefore become a corporate imperative *(Institute of Directors of South Africa, 2009; Kerr & Murthy, 2013).* The lack effective internal IT controls is the primary root cause for financial misstatements *(Benaroch, Chernobai. & Goldstein, 2012).* However, the potential consequences go beyond financial reporting and includes loss of revenue, operational disruptions, non-compliance to legislation, lack of investor confidence, reputational damage and the cost of recovery *(Lunardi, Becker, Maçada & Dolci, 2014).* In addition, organisations have become aware of the need for governance of their data assets, due to the growth of digitised data inside and outside of the organisational boundary and the increase in the possibilities to access this data *(Kooper, Maes & Lindgreen, 2011).* The rising interest in IT governance is also due to compliance initiatives (e.g. Sarbanes-Oxley and Basel III), and the acknowledgement that IT is an increasingly important element of organisations' products and services *(Weill & Ross, 2004; Gheorghe, 2010; Bowen, Chung & Rohde, 2007).*

Governance is generally considered as a hierarchical framework for guidelines, policies, responsibilities, and procedures to ensure a certain level of control within an organisation *(Kooper, Maes & Lindgreen, 2011).* ISO 38500 defines the ***corporate governance of IT*** as the system by which the current and future use of IT is directed and controlled. It involves evaluating, monitoring and directing the use of IT to support the organisation and to achieve plans *(ISO, 2008).* The King III Code further defines IT governance as a framework that supports effective and efficient management of IT resources to facilitate the achievement of a company's strategic objectives. It includes the governance of the information and the governance of the underlying technology *(Institute of Directors of South Africa, 2009).* IT governance specifies the decision rights and accountability framework to encourage desirable behaviour in the use of IT *(Weill & Ross, 2004).* Value creation and risk management are the two main IT governance objectives of an enterprise *(IT Governance Institute, 2012).* Notwithstanding the variety of IT governance definitions, the "golden thread" is that IT should sustain the organisation's objectives *(Gheorghe, 2010).*

IT governance is a subset discipline of corporate governance, focused on information technology and information assets *(Kooper, Maes & Lindgreen, 2011; Well & Ross, 2004).* It should follow the principles of corporate governance *(Gheorghe, 2010).* Governance focuses on the role of the board and directors in representing and protecting the interest of shareholders *(Kooper, Maes & Lindgreen, 2011).* IT governance is also defined as the organisational capacity exercised by the board, executive management and IT management to control the formulation and implementation of the IT strategy *(van Grembergen, 2002).* It involves all levels in the organisation, as it takes place at both the macro level (i.e. board) and the micro level (management) of the organisation *(von Solms & von Solms, 2006).* The board of directors of the organisation is ultimately accountable for IT governance and should delegate the responsibility to the management of the organisation to implement it *(Institute of Directors of South Africa, 2009).* IT governance should not be considered in isolation, because IT is linked to other key enterprise assets (e.g. financial, human, intellectual property) and might even share mechanisms with other governance processes *(Weill & Ross, 2004; Gheorghe, 2010).* Information security governance, as part of IT governance, is also a corporate governance responsibility and a subset of corporate governance *(von Solms & von Solms, 2006).*

An IT governance framework is: 1) a basic conceptual structure used to solve or address complex issues; 2) an enabler of governance; and 3) a set of concepts, assumptions and practices that define how something can be approached or understood, the relationships

between the entities involved, the roles of those involved, and the boundaries *(IT Governance Institute, 2012).* Numerous frameworks, codes, standards and guidelines have been developed through organisations such the IT Governance Institute (ITGI), Information Systems Audit and Control Association (ISACA), International Standards Organisation (ISO) and the Open Compliance and Ethics Group (OCEG) *(Leill-Cock, Graham & Hill, 2009).*

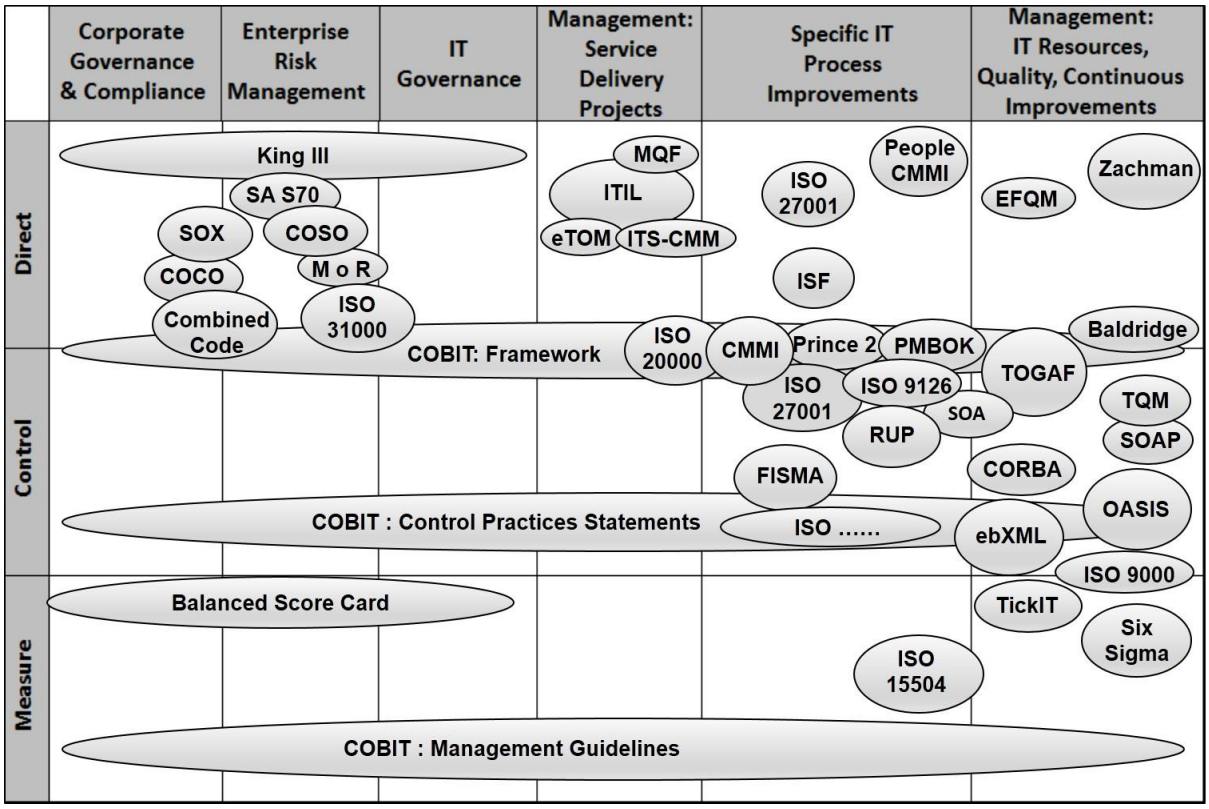


Figure 2-6 IT Governance and Control Frameworks, Codes and Standards (Leill-Cock, Graham & Hill, 2009)

An effective IT governance framework should include the relevant structures, processes and outcome metrics to enable IT to deliver value to the business and to mitigate IT risk *(Bowen, Chung & Rohde, 2007).* There is no single framework recognised as the clear market leader, or "best" IT governance framework *(Verhoef, 2007; Bowen, Chung & Rohde, 2007).* Each of the overlapping and competing frameworks, codes, standards and guidelines has its own purpose, strengths, weaknesses and focus *(Leill-Cock, Graham & Hill, 2009; Gheorghe, 2010).*

Business objectives or strategy is the factor that most heavily influences the implementation of IT governance practices *(IT Governance Institute, 2011).* For example, organisations within the manufacturing, retail and public sectors are less likely to implement IT governance than in the financial services or IT / telecoms sectors *(ISACA, 2011).* The 2012 global ISACA IT governance survey found that 58% of organisations use a formal IT governance framework or

standard, and that the key drivers for implementing IT governance relate primarily to: 1) value delivery through the alignment of IT to the business; 2) the ability to support changes in the business; and 3) achieving a balance between innovation and risk to improve returns *(ISACA, 2012).* However, 30% of the respondents were from the financial services (e.g. financial, banking, insurance) sector and only 3% from the utilities sector. Overall, the administrative intensive sectors, such as insurance, banking, public accounting, legal, real estate, education and marketing represented 46% of the respondents. Only 12% of the respondents represented the infrastructure asset intensive sectors, including manufacturing, mining, utilities, construction / engineering and transport *(ISACA, 2012).* This survey therefore does not adequately reflect the IT governance situation within infrastructure asset intensive or industrial organisations.

IT governance can be performed on a ***statutory (compliance) basis***, or as a code of principles and practices, or a combination of the two *(Verhoef, 2007; Institute of Directors of South Africa, 2009).* The key drivers for implementing IT governance in South African organisations are primarily related to compliance to regulation, risk reduction and the improvement of operational controls *(Chitambala, 2006).* The rising interest in IT governance globally is also partially due to compliance initiatives, such as Sarbanes-Oxley and Basel III *(Kerr & Murthy, 2013; Bowen, Chung & Rohde, 2007).* A number of highly publicised cases of corporate fraud, such as Enron and WorldCom, resulted in increased attention to governance and internal controls *(Kerr & Murthy, 2013).* The primary reason for the majority of the IT governance adoptions in Brazil between 2004 and 2005 was to conform to the requirements of the Sarbanes-Oxley Act, which is obligatory for companies who want to negotiate shares on the New York Stock Exchange *(Lunardi, Becker, Maçada & Dolci, 2014).* This included financial organisations and industrial organisations (e.g. oil and gas, utilities, and transport) *(Lunardi, Becker, Maçada & Dolci, 2014).* The King III Code adopted a "comply or explain" regime, rather than the "comply or else" regime adopted by the Sarbanes-Oxley Act *(Institute of Directors of South Africa, 2009).*

A 5-level process capability ***maturity model*** is applied to IT governance, in order to assess the current capability and determine the performance of the IT governance and IT management processes, as well as to set the target maturity and identify the improvement required to close the gap *(IT Governance Institute, 2007 & 2012).* According to a 2011 global status report on IT governance, there is a wide distribution across the 5 levels, with the majority of organisations having a level of maturity between levels 1 and 3 (i.e. between ad-hoc and

defined) *(IT Governance Institute, 2011).* The survey also found that: 1) there is a close correlation between the importance of IT to the organisation and its IT governance maturity level, as those organisations that consider IT to be important for the business generally have a higher level of IT governance maturity; and 2) there is a close correlation between organisation size and IT governance maturity, as larger organisations tend to be more mature in terms of IT governance than smaller organisations *(IT Governance Institute, 2011).*

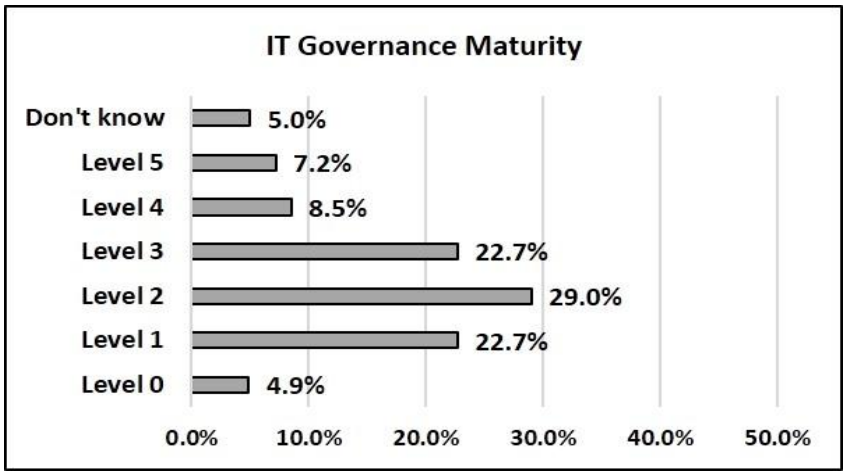


Figure 2-7 IT Governance Maturity (IT Governance Institute, 2011)

The cost and effort required to aim at a high level of IT governance maturity should be considered, versus the expected value that such a capability will deliver to the organisation *(IT Governance Institute, 2011).* The optimal IT governance and management maturity level will be different for every organisation and the context of the organisation needs to be considered *(IT Governance Institute, 2012).* It should be appropriate and applicable to the IT organisation's size, role and legal obligations *(Liell-Cock, Graham & Hill, 2009).*

There is a growing tendency towards ***internally developed frameworks*** that use a combination of practices and guidelines from different frameworks (*ISACA, 2011; Lunardi, Becker, Maçada & Dolci, 2014).* Organisations tend to look at multiple sources for guidance, rather than a "one size fits all" approach, because IT needs to respond to the unique environments within which it operates *(Verhoef, 2007; Bowen, Chung & Rohde, 2007).* There are also meta frameworks, such as the Calder-Moir Framework of Frameworks. These meta frameworks assist organisations to use overlapping and competing frameworks and standards to deploy the suitable and relevant practices contained in these frameworks and standards *(ISACA, 2011).* Such frameworks obtain the benefits of each without incorporating irrelevant details *(Lunardi, Becker, Maçada & Dolci, 2014).* One such example can be found in the South African public service. The South African government published an IT governance framework for use within

the government *(Department of Public Service and Administration, 2012).* The framework consists of four layers, namely: 1) corporate governance; 2) the corporate governance of ICT, which focuses on evaluating, directing and monitoring the use of ICT to support the organisation; 3) governance of ICT, which focuses on the effective and efficient management of IT resources to facilitate the achievement of company strategic objectives; and 4) operational management of ICT.

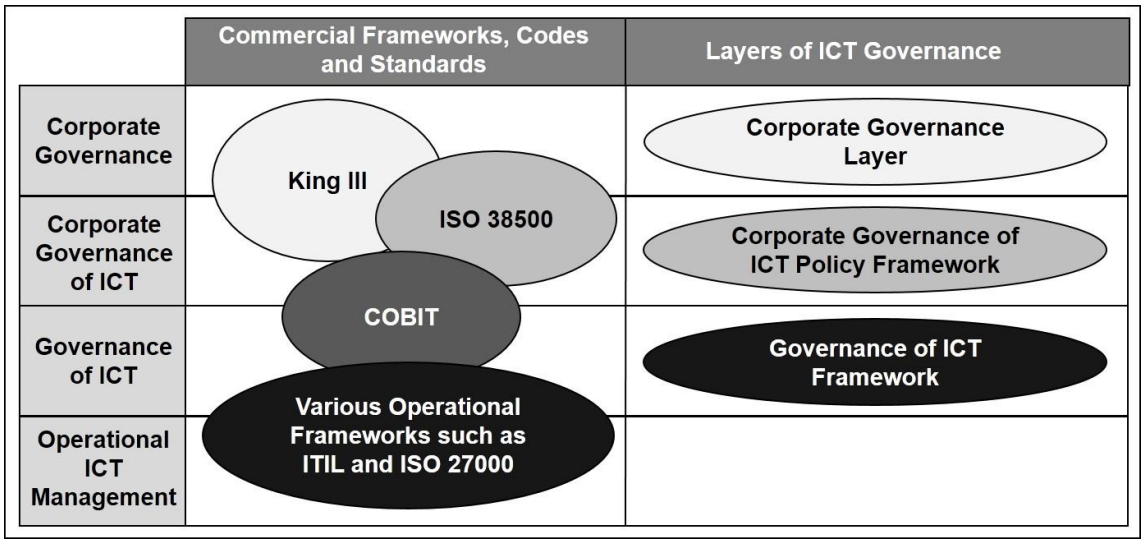


Figure 2-8 South African Government IT Governance Framework (Department of Public Service and Administration, 2012)

It uses a combination of COBIT, ITIL, the King III Code, ISO 38500 and ISO 27000 across the 4 layers. All organs / entities of state are required to comply with the corporate governance of ICT layer of the framework *(Department of Public Service and Administration, 2012).*

The ***organisational structure of IT governance*** mechanisms is an important component of IT governance *(Weill & Ross, 2004; van Grembergen, de Haes & Guldenstops, 2004).* Such structures can be categorised as centralised, decentralised, or federal *(Sambamurthy & Zmud, 1999; Prasad, Heales & Green, 2010).* An ***IT steering committee*** is the primary and most prominent governance structure for IT investments and ongoing IT operations *(Bowen, Chung & Rohde, 2007).* Effective IT governance depends to a large extent on an effective co-created IT steering committee and operational committees *(Prasad, Green & Heales, 2012).* These committees will ensure continued top management support for IT initiatives, as well as shared organisational knowledge in terms of IT strategies, policies and initiatives *(Prasad, Green & Heales, 2012).* The IT steering committee is a lateral IT-related organisational coordinating structure that embraces an appropriate mix and balance of participation *(Prasad, Heales & Green, 2010).* This includes participation from business and digital functions, as well as

participation from different levels of the organisational hierarchy *(Prasad, Heales & Green, 2010).* The key roles and responsibilities of the IT steering committee in support of effective IT governance, include: 1) translating business and strategic goals into actionable plans; 2) IT strategy definition; 3) IT policy setting; 4) organisation-wide coordination of IT resources; 5) IT project portfolio management and oversight; 6) IT performance reviews; 7) compliance with relevant regulations; 8) enterprise architecture and standards decisions; 9) IT risk management; and 10) IT related collaboration and communication to ensure a common understanding of strategic business needs, IT strategies, IT policies, IT performance and IT governance amongst all parties *(IT Governance Institute, 2007; Nolan, 2005; Bowen, Chung & Rohde, 2007; Weill & Ross, 2004).* The benefits of an effective IT steering committee do not only remain at a strategic level, but flow down to the operational business processes *(Prasad, Green & Heales, 2012).*

IT governance processes is one of the enablers of IT governance and should be part of the IT governance framework to support the IT governance structures *(Bowen, Chung & Rohde, 2007; IT Governance Institute, 2012).* These processes are used by the organisation to govern and manage IT *(Kaplan, 2005).* The primary purpose of IT governance processes is to embed IT governance accountability into the organisations *(Bowen, Chung & Rohde, 2007).* IT is governed through three main tasks, namely: 1) evaluate the current and future use of IT, including strategies, proposals and supply arrangements; 2) direct preparation and implementation of plans and policies to ensure that the use of IT meets the business objectives; and 3) monitor conformance to policies, and performance against the plans *(ISO, 2008*). For IT governance to be effective, organisations should monitor their IT performance and overall value to the business through appropriate measurement systems *(Schawrtz & Hirschheim, 2003).* IT governance outcome metrics assess both IT governance structures and processes to ensure that the desired results are being obtained *(Bowen, Chung & Rohde, 2007).*

COBIT 5.1 specifies two separate disciplines, or levels, that are both required to provide a ***holistic approach to IT governance***, namely the governance of IT and the management of IT *(IT Governance Institute, 2012).* These 2 disciplines are both important and are associated, but they remain different, serve different purposes and include different types of activities *(Gheorghe, 2010; IT Governance Institute, 2012).* IT management is in charge with providing effective IT services and products *(Gheorghe, 2010).* It plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives *(IT Governance Institute, 2012).*

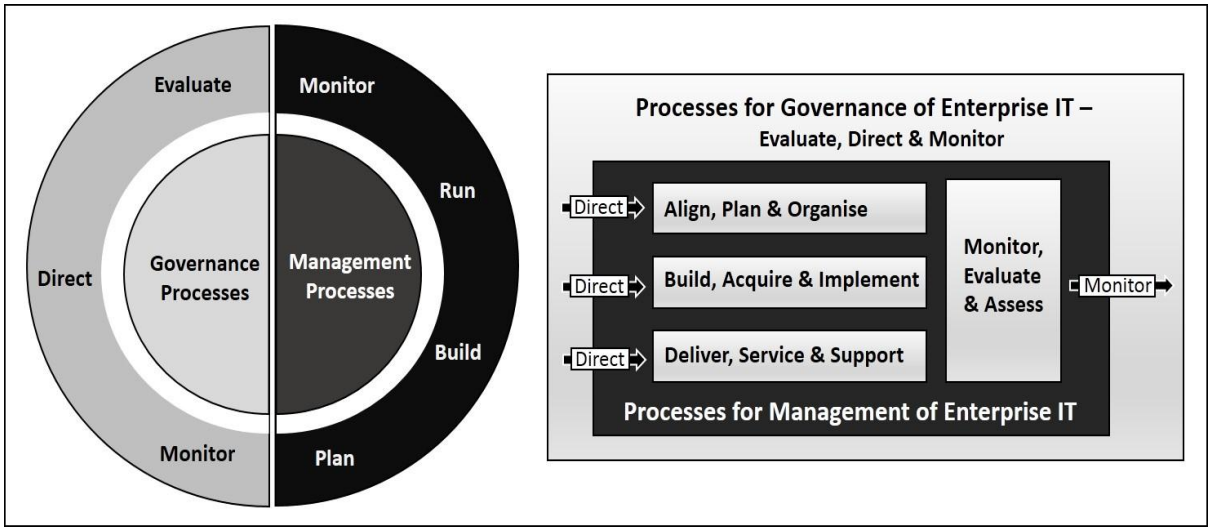


Figure 2-9 Governance and Management Processes (IT Governance Institute, 2012)

IT governance is much broader and focuses on performing and transforming IT to meet the demands of the business and its customers *(Gheorghe, 2010).* It deals with governance objectives (e.g. value delivery, risk optimisation, and resource optimisation) and includes activities aimed at evaluating strategic options, providing direction to IT and monitoring the outcome *(IT Governance Institute, 2012).*

Internal control, or management control, is a process designed to provide reasonable assurance about the attainment of organisational objectives *(COSO, 1994).* The collection of IT-specific internal process controls is an important component of an organisation's arsenal of internal controls *(Benaroch, Chernobai & Goldstein, 2012).* They are the management, operational and technical safeguards prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information *(Benaroch, Chernobai & Goldstein, 2012).* A suitable and appropriate internal IT control framework should contain a clear link between the company's risk management and independent assurance processes *(IT Governance Institute, 2011).* The purpose of internal IT control is to demonstrate reasonable assurance that security risks are kept to an acceptable level *(Spears, Barki & Barton, 2013).* It reduces decision risk by improving confidence in the quality of the information used *(Port & Wilf, 2014).* Compliance also reduces risk by improving confidence in the quality of the software, but assurance is more than compliance with standards *(Port & Wilf, 2014).* A risk-based approach versus a pure compliance-based approach is more effective, because it allows the assurance provider to determine whether controls are effective in managing the associated risks *(Institute of Directors of South Africa, 2009).* The top 5 most important control

processes for IT, as defined in COBIT 4.1 are: 1) ensure system security; 2) manage changes; 3) assess risk; 4) manage data; and 5) assess internal control adequacy *(Kerr & Murthy, 2013).*

Risk management is a key concept of IT governance and operational process controls *(Tohidi, 2011).* Risk is the potential that a given threat will exploit vulnerabilities of an asset, or group of assets, to cause loss or damage to the asset *(Zhiwei & Zhongyuan, 2012).* Risk management is the process to identify and assess risk and to apply methods to reduce it to an acceptable level *(Tohidi, 2011).* It aims to identify, measure and control uncertain events and to assist organisations to better manage risks associated with their missions *(Tohidi, 2011).* It also enables IT managers to balance the operational and economic costs of achieving the IT mission. *(Tohidi, 2011).* Risk assessment is at the core of risk management and is the means by which risks are identified and evaluated to justify controls *(Zhiwei & Zhongyuan, 2012).*

2.7. Transition and Change Management

The implementation of any IT-enabled change, including the implementation of an IT governance or control framework, requires significant ***cultural and behavioural change*** *(IT Governance Institute, 2012).* Apart from the business objectives, the culture of the organisation, its way of working and human factors have the most influence on the implementation of IT governance practices *(ISACA, 2012).* The culture of an organisation is defined as a long-lived set of values, beliefs, attitudes and assumptions, which are thought to affect behaviour and performance *(Johnson, 2010; Mearns, Whitaker & Flin, 2003; Clarke, 2006).* The main challenges and barriers encountered in implementing IT governance mechanisms are change management, communication issues, and trying to do too much at once *(ISACA, 2012).*

Change management is defined as a structured approach to transitioning individuals, teams, and organisations from a current state to a desired future state *(East, 2011).* It is a hybrid approach that combines a mechanical way of looking at change with the human focus required to help people on the journey *(East, 2011).* It addresses the "hard" side of change management, including the frequency of formal reviews of change projects, the formal commitment of top management and the effort required from employees over and above their normal duties to implement the change *(Sirkin, Keenan & Jackson, 2005).*

There are three types of organisational change, namely:

Type	Description
Developmental change	Where the new state is a prescribed enhancement of the old state.
Transitional change	Where the current state is replaced with something entirely different.
Transformational change	Where the change from one state to another is so radical that it requires a shift in culture, behaviour and mind-set.

Table 2-6 Types of Organisational Change (Sirkin, Keenan & Jackson, 2005)

Transition management must address three dimensions, in order to be successful, namely: 1) the content of the change (i.e. what needs to be changed); 2) the people who will implement the change or be impacted by the change; and 3) the process of how the change will be achieved *(Anderson & Anderson, 2001).* Change can be achieved either as a single large scale change, such as transformation, or as a collection of smaller incremental adjustments *(East, 2011).* It can also be planned change that requires formalisation, or it can be emergent changes that take place over time through continual learning and adaptation *(van der Voet, 2014).* The Kurt Lewin model is a model for changing the culture of an organisation. It consists of three stages namely:

Stages	Description
Unfreezing	Determine the need for change, assess readiness for change and prepare for change.
Changing	Identify the change mechanisms, engage people and plan the migration.
Refreezing	Apply rewards, maintain the change and avoid relapse.

Table 2-7 Kurt Lewin Model (Conger, Spreitzer & Lawler, 1999)

The Kotter approach to managing change consists of 8 sequential steps, or change accelerators, that will ensure that the most prominent reasons for change initiative failures are addressed *(Kotter, 2012).* These 8 steps are: 1) establish a sense of urgency by helping others to see the need for change; 2) form the guiding coalition to lead the change effort; 3) develop a change vision to help direct the change effort; 4) communicate the vision for buy-in; 5) empower broad-based action by removing change obstacles, building trust and encouraging risk-taking and non-traditional ideas; 6) generate short-term wins to make achievements visible; 7) never letting up (don't let up) and re-invigorate the process with new projects; and 8) institutionalise

changes ("make it stick") by articulating the connections between the new behaviour and organisational success *(Kotter & Schlesinger, 2008; Kotter, 2012).*

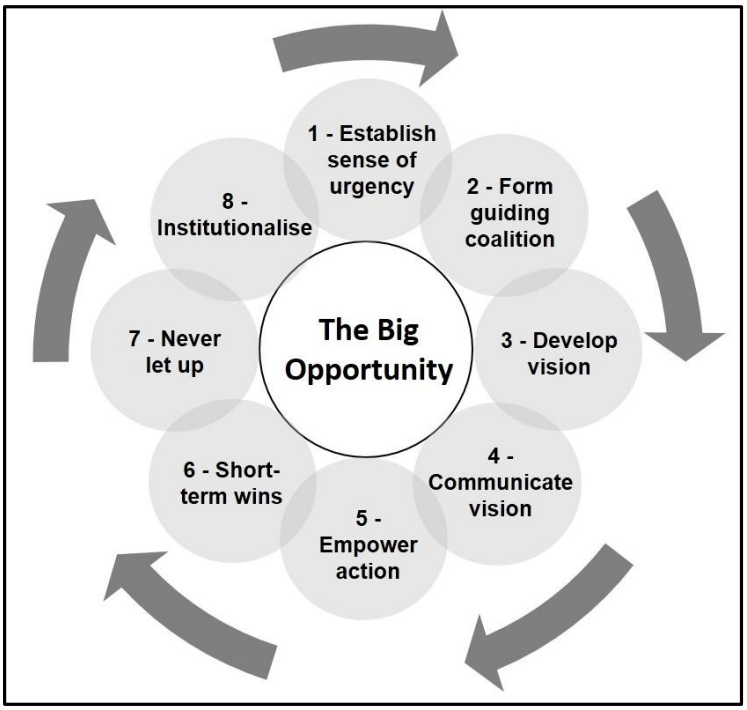


Figure 2-10 Kotter Change Process (Kotter, 2012)

There are a number of ***additional overlapping concepts and disciplines*** that form part of the overall journey of implementing a new way of thinking and working in an organisation. These include roadmaps, program management, business re-engineering, organisational development and maturity models. ***Program management*** is the centralised coordinated management of a program to achieve the program's strategic objectives and benefits *(PMI, 2013).* ***Business (process) re-engineering*** is the radical redesign of strategic, value-added business processes, including the systems, policies, and organisational structures that support the process, in order to optimise the work flows and productivity in an organisation *(Manganelli & Klein, 1994).* ***Organisational development*** is a system-wide and value-based collaborative process of applying behavioural science knowledge to the development and improvement of organisational features, such as the strategies, structures, processes, people and cultures *(Anderson & Anderson, 2001).*

A ***maturity model*** consists of a sequence of maturity levels that represents an anticipated or desired evolutionary path as discrete stages *(Becker, Knackstedt & Pöppelbuß, 2009).* It describes the state of "perfection" or "completeness" of certain capabilities *(Wendler, 2012).* The term "maturity" also relates to the degree of formality and optimisation of processes, from

ad-hoc practices to active optimisation of the processes *(Wendler, 2012)*. A maturity model can be used to determine the maturity of the current practices, set a target maturity, and identify the improvements required to reach the target maturity *(IT Governance Institute, 2012).* The same principles of the initial 5-scale software engineering capability maturity model *(Humphrey, 1989)* are also applied to more than 22 disciplines such as IT governance, asset management, enterprise architecture, project management, sustainability, knowledge management, IT security, process management and collaboration *(Wendler, 2012; Lange & Kasan, 2014; Pilling, 2010; Ross, 2004; Kluth, Jäger, Schatz & Baurenhansl, 2014; Kyriakidou, Michalakelis & Sphicopoulos, 2013; Šaša & Krisper, 2011; Spears, Barki & Barton, 2013).*

Roadmaps are applied as a tool for long-term strategy or business model implementation, new product development, consensus seeking, transition steering and program governance purposes *(McDowall, 2012; Leitão, Cunha, Valente & Marques, 2013; Oliviera & Rozenfeld, 2010).* The implementation of IT governance is not a once-off project *(IT Governance Institute, 2012).* Whilst some improvements may be quick wins, others are longer term initiatives *(Kotter, 2012; IT Governance Institute, 2012).* Quick wins are directed at those areas where the value-add can be clearly demonstrated, in order to assist in obtaining and maintaining buy-in from senior management, as well as to provide the platform for further changes *(Kotter, 2012).* The implementation, or transition, roadmap must be appropriate and the underlying analysis must be of an acceptable quality *(McDowall, 2012; Georghiou & Keenan, 2006).* A transition roadmap should satisfy the following requirements:

Requirement	Description
Adaptability	The roadmap must be consistent with reflexive, adaptive management. The process must involve periodic reviews and updates, as well as adjustments, based on reflection and learning, instead of a once-off development. This will ensure responsiveness to changes in the environment, a change in the future scenario(s), and new opportunities, whilst still having an agreed vision.
Credibility	The roadmap must define a future state that is credible, plausible and persuasive. It must be based on sound analysis, draw on the appropriate expertise and knowledge within the organisation. It must have secured participation and commitment from key stakeholders. Credibility and desirability provide legitimacy to the roadmap.
Desirability	The roadmap must be defensible as a good and desirable choice for the organisation. The transition must satisfy and achieve the organisation's goals and vision related to the research topic. It must have a clear justification for the chosen path and it must be set in a transparent and inclusive manner.

Requirement	Description
Utility	The roadmap must be useful or fit for purpose. It must provide a coherent future with clear targets and priorities. It must be appropriate for the organisation based on the characteristics of the organisation.

Table 2-8 Roadmap Requirements (Adapted from McDowall, 2012)

One of the examples of an implementation roadmap, or life cycle, for the implementation of an IT governance or control framework is defined in COBIT 5 *(IT Governance Institute, 2012).* The COBIT 5 implementation approach includes: 1) a program management work stream to govern and manage the initiative; 2) a change work stream to address the behavioural and culture aspects; and 3) a continuous improvement life cycle, because this is not a once-off project *(IT Governance Institute, 2012).*

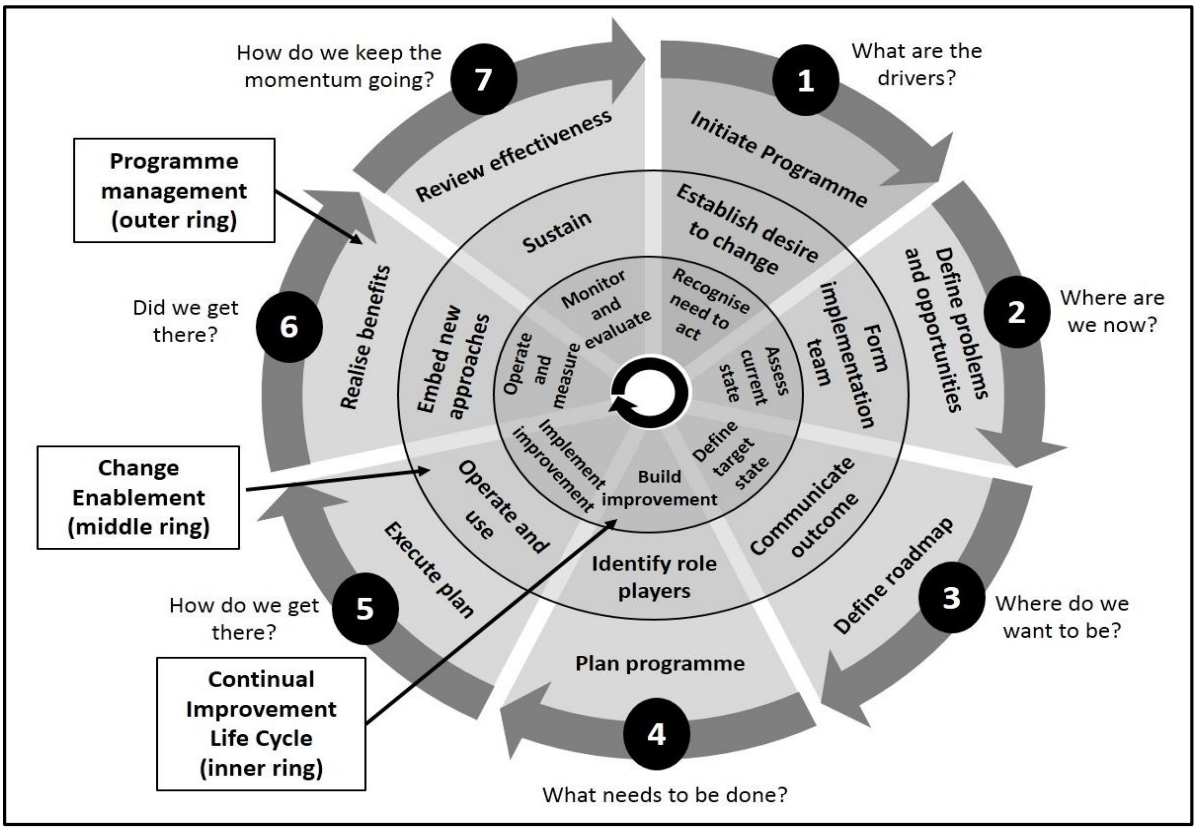


Figure 2-11 IT Governance Implementation Life Cycle (IT Governance Institute, 2012)

A change process model or framework is ***not a cookbook*** for a successful transition *(Anderson & Anderson, 2001).* An organisation should select the appropriate roadmap and tailor it to fit the organisation and the nature of the change *(Kotter & Schlesinger, 2008; East, 2011; Anderson & Anderson, 2001).* It should tailor the roadmap based on the organisation's risk appetite, capabilities and resource capacity, industry practices, current level of maturity, business plans and strategies *(IT Governance Institute, 2012).* The journey of transitional

change is not a straight line, due to some degree of uncertainty and a shifting target state *(Anderson & Anderson, 2001).* Some degree of flexibility and "course corrections" will be required along this path *(Anderson & Anderson, 2001).*

2.8. Observations

Observations that relate to the research topic and influenced the design of the artefact were made by the researcher, based on the literature review. These observations are presented in this section.

Infrastructure asset management is becoming globally recognised as an important discipline. It is becoming more formalised and sophisticated. It requires quality asset information from across the digital landscape to be utilised to support evidence-based group strategic asset decision making. Asset information is increasing in volume and variety and the developments in infrastructure asset condition assessment technology is contributing to this trend. The management of asset information also includes related disciplines and activities, such as information security, data quality management, information governance and records management, in order to effectively enable infrastructure asset management. Digital technology has been converging for some time and the integration of IT and control systems is increasing. Enterprise architecture remains an important discipline to manage complexity and change in an organisation. This includes the current and future information, technical and business architecture, as well as cross-domain architectures, such as information security. IT governance is recognised as an important discipline for organisations that consider IT to be important. It is unclear to what extent IT governance has been applied in asset intensive organisations or to control systems. There is a trend to define and implement internal IT governance frameworks by tailoring one or more framework(s) based on the characteristics of the organisation. Compliance to a standard or legislation is an important reason for some organisations to implement IT governance rather than a risk-based approach. There is a trend to apply a holistic approach to IT governance. This holistic approach includes both the governance and operational process control, or management, levels. It is recognised that the implementation of IT governance is a change initiative, which is exposed to the normal change management related risks. Such an implementation approach also makes use of associated disciplines and tools, such as project and program management, maturity models and roadmaps. These are tailored for the specific discipline and organisation to ensure a successful transition during this long and difficult road.

Chapter 3 - Rand Water as Base Case

The purpose of this chapter is to present the base case for the research, namely Rand Water. The minimum relevant characteristics of Rand Water will be described to provide the context for the rest of the research. It includes a description of the Rand Water organisation, its infrastructure assets, asset management practices and digital technology landscape.

3.1 Rand Water

Scarcity of water was a problem in 1886 when gold was discovered in the Witwatersrand ("Ridge of white waters") area of South Africa. It was soon realised that water was needed for the processing of gold ore, the secondary industries and the ever growing population in the area. The first sources of water at this time were boreholes and the springs surrounding Johannesburg. Water was very expensive at that time and the existing water sources became inadequate. The population of the Witwatersrand grew from 100,000 in 1896 to 500,000 in 1913. This is a 500% increase in less than two decades. The need to establish a single public entity to supply water to the entire Witwatersrand was identified. The Rand Water Board, now called Rand Water, was established on 8 May 1903 and commenced with full operations in 1905. The need to use water from the Vaal River, as a sustainable source of water, was also recognised as inevitable. Phase one of the Vaal river scheme went into production in 1923 *(Rand Water, 2003).*

Rand Water experienced exponential ***growth*** since it was established. In 1906 the annual daily consumption of water was approximately 11 Mega litres per day (Ml/d). By 1944 the area of service was enlarged to include the whole Pretoria-Witwatersrand-Vereeniging area, which is today known as the Gauteng Province of South Africa *(Rand Water, 2003).* The service area was subsequently increased again to include the Rustenburg area in the North West province and the surrounding platinum mines, as well as selected areas in the Mpumalanga and Free State provinces *(Rand Water, 2014).* Water provision to a number of strategic state owned entities were added to the customer base of Rand Water, including the national Iron and Steel Corporation of South Africa (ISCOR), the national electricity utility (Eskom) and South African Synthetic Oil Limited (SASOL) *(Rand Water, 2003).* As at 2014, Rand Water is the largest water utility in Africa and one of the largest in the southern hemisphere. It has an annual revenue of ZAR 8.67 billion. Rand Water provides more than 12 million people in the

economic heartland of South Arica with 4,183 Ml/d of world-class potable water that meets the nationally accredited water quality standards (i.e. SANS 241:2005) *(Rand Water, 2014).*

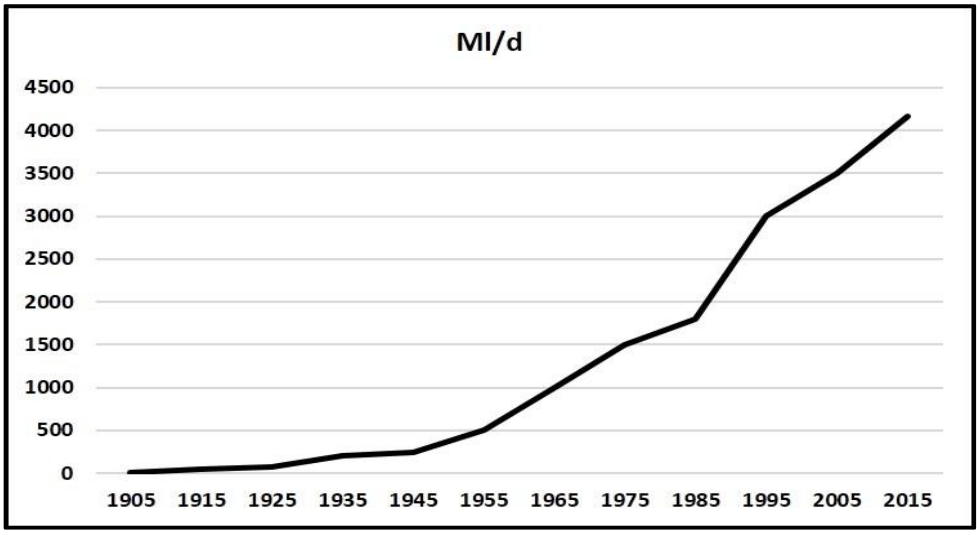


Figure 3-1 Rand Water Volume Growth (Rand Water, 2003; Rand Water, 2014)

The water supply volume increased four-fold from 1965 to 2014 *(Rand Water, 2003; Rand Water, 2014).* The water demand within the current service area of Rand Water is forecasted to be approximately 5,550 Ml/d by 2030 *(Rand Water, 2014).* One of the strategic goals of Rand Water is growth. The objectives of the growth strategy include the diversification of Rand Water's income streams and the enlargement of the service area due to the envisaged institutional reform of the South African water sector *(Rand Water, 2014).*

The primary ***service*** of Rand Water is the supply of bulk potable water. This is considered to be an essential service in the South African context. The primary Rand Water supply area, Gauteng, generates 60% of South Africa's Gross Domestic Product *(Rand Water, 2014).*

Figure 3-2 Rand Water Service Area (Rand Water, 2013)

Bulk potable water is also provided to parts of the three neighbouring provinces, namely the Free State, North West and Mpumalanga. Rand Water's secondary services include bulk sanitation, bulk industrial quality water, bottled water, water demand management and catchment management.

Rand Water has a wide range of ***stakeholders*** to be considered. The key stakeholders include the Rand Water shareholder (i.e. Department of Water Affairs and Sanitation), investors, board of directors, employees, provincial legislature, suppliers, tertiary institutions, National Treasury, the auditor general, civil society organisations, the South African Local Government Association, the media and Rand Water's customers. Rand Water employs 3,869 permanent staff members across its area of service. Rand Water's customers include municipalities and direct customers in the industrial and mining sectors.

To ensure that Rand Water remains Africa's leading water utility, the ***vision and mission*** of Rand Water are as follows:

> **Vision:** To be a provider of sustainable, universally competitive water and sanitation solutions for Africa.
>
> **Mission:** To deliver and supply world class affordable, reliable, and good quality water and related services to all stakeholders through: 1) safe, efficient, sustainable and innovative business practices; 2) empowered employees; mutually beneficial strategic relationships; and 3) legislative compliance and best practice.

In line with the vision and mission, the Rand Water ***strategic goals*** and the underlying objectives will focus and direct the business activities of the organisation over the planning period. These are:

Strategic Goal	Associated Objectives
Achieve Growth	To ensure that Rand Water's infrastructure meets current and future demand; promote growth through new areas of supply; and promote growth through new product streams.
Achieve a High Performance Culture	To build integrity within the organisation; build employee morale and satisfaction; build internal skills and capacity; retain employees through an attractive environment; transform Rand Water's employee profile to reflect the demographics of the area of supply; provide required assurance at board level; and retain Rand Water's institutional knowledge.

Strategic Goal	Associated Objectives
Achieve Operational Integrity and Use Best Fit Technology	To ensure compliance to all statutory and regulatory requirements; promote safety, health, the environment and quality; increase protection of Rand Water's assets and personnel; ensure continuous supply of water to customers; ensure the quality and reliability of Rand Water assets; effectively co-ordinate and utilise Rand Water's information and communication technology and knowledge management; maintain the quality of water; and improve internal processes within the Rand Water Group.
Maintain Financial Health and Sustainability	To promote prudent financial management; achieve optimal investment portfolio performance; mitigate all financial risk for the Rand Water Group; ensure that assets are fully utilised; and ensure that the tariff is determined accurately from Rand Water's environment.
Positively Engage Stakeholder Base	To promote and implement initiatives that have a socio-economic development impact; reduce legal risk and thereby minimise the financial and reputational impact on Rand Water; improve awareness of Rand Water with external stakeholders; and respond appropriately to Rand Water's environment.

Table 3-1 Rand Water Strategic Goals and Objectives

Rand Water is a State Owned Entity, established in terms of the Water Services Act No. 108 of 1997. The Government of the Republic of South Africa, through the Department of Water Affairs and Sanitation, duly represented by the Minister, is the sole shareholder of Rand Water *(Rand Water, 2013).* A board of executive and non-executive directors is the governing body and accounting authority of Rand Water. Various sub-committees exist to assist the board in discharging its duties, including an audit committee, risk committee, and capital investment committee *(Rand Water, 2014).*

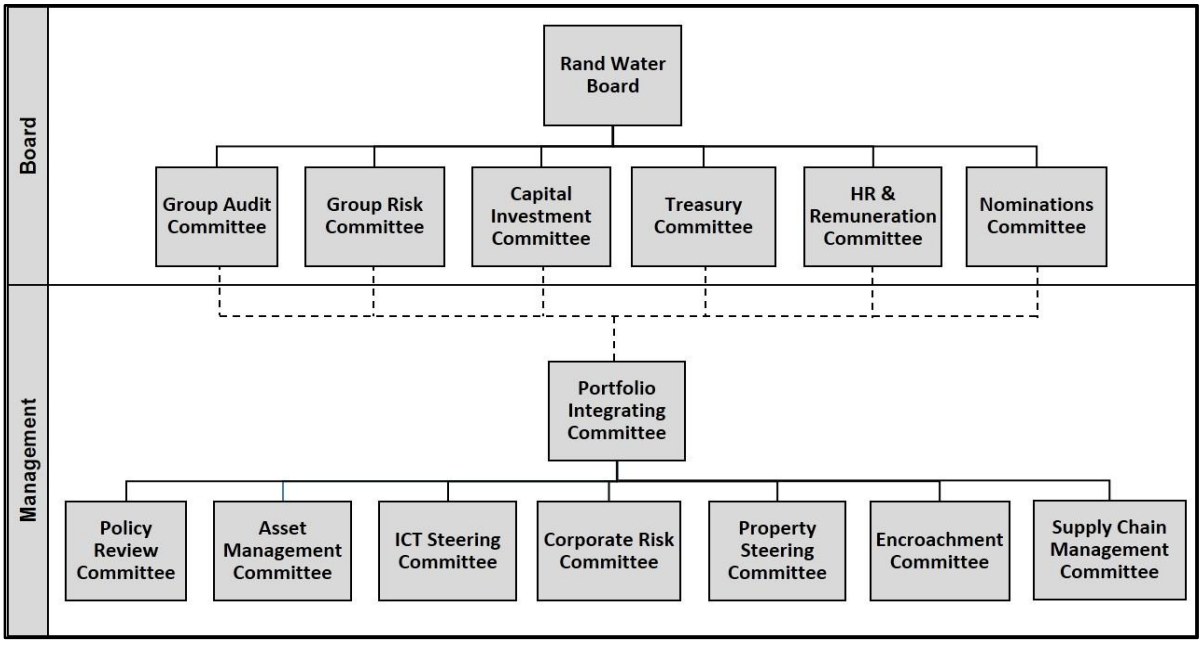


Figure 3-3 Rand Water Governance Structure (Rand Water, 2014)

An executive management committee, called the Portfolio Integrating Committee, reports to the board. It is supported by a number of sub-committees, such as the policy review committee, corporate risk committee, supply chain management committee, asset management committee and ICT / digital steering committee *(Rand Water, 2014).* The ICT steering committee was established in 2007. It initially focused only on IT and excluded control systems. The ***organisational structure*** of the organisation consists of 6 portfolios, each headed up by an executive, or portfolio head. The portfolios and the functions within each portfolio are as follows:

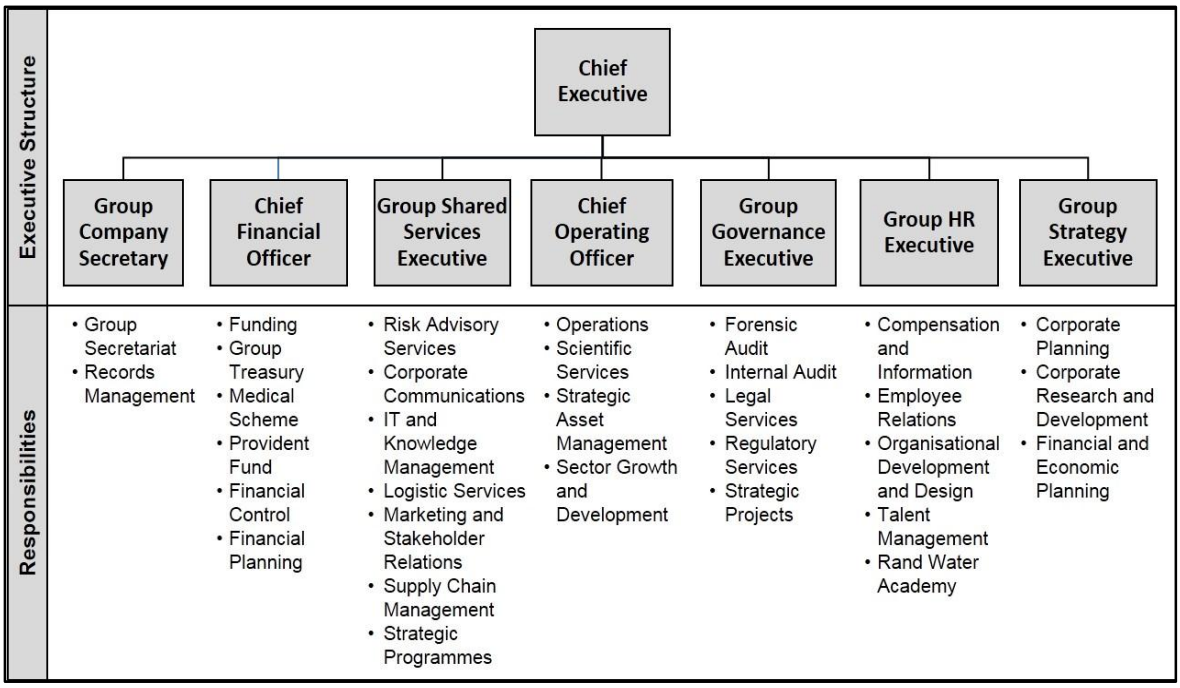


Figure 3-4 Rand Water Organisational Structure (Rand Water, 2014)

Rand Water operates in a ***heavily regulated environment***. Some of the key relevant legislation are the National Water Act, Water Services Act, Public Finance Management Act, National Key Point Act, National Environmental Management Act, Promotion of Access to Information Act and the Protection of Personal Information Act. In addition, Rand Water decided to comply with a number of codes and standards, such as: 1) quality management (ISO 9001); 2) environmental management (ISO 14001); 3) water quality (e.g. South African National Standards 241 and the World Health Organisation's drinking water quality guidelines); 4) accounting (i.e. South African Statements of Generally Accepted Accounting Practice); 5) occupational health and safety (i.e. OHSAS 18001: 2005 South African Bureau of Standards certification); 6) asset management (i.e. ISO 55000); and 7) governance (i.e. King Report on Corporate Governance from the Institute of Directors of South Africa). This includes the IT

governance principles of the King III code. Rand Water further developed and implemented corporate governance, risk management, delegation of authority, compliance and combined assurance frameworks *(Rand Water, 2014).*

Rand Water has been able to deliver excellent quality water at a reasonable cost for more than a century, whilst facing many significant ***problems*** during this period. Such problems include 1) sink holes impacting the pipelines; 2) an explosion in the population in the Rand Water area of service; 3) two world wars that prevented the raising of the necessary capital for asset infrastructure projects; 4) the great South African depression of the 1930's; 5) floods in Rand Water's primary catchment area; 6) droughts caused by the Kalahari high pressure cell and the El Niño phenomenon over the Pacific ocean; 7) the arid nature of South Africa with an average evaporation rate that is higher than the average precipitation rate; 8) electricity shortages; and 9) infrastructure asset failure *(Rand Water, 2003).* The following are some of the ***top ten strategic risks*** that could have a negative impact on Rand Water achieving its strategic goals: 1) deterioration in raw water quality; 2) encroachment over pipeline servitudes and properties; 3) optimisation and age of critical installations; 4) non-revenue water in the municipal system; 5) legal compliance; 6) capacity to supply or inability to supply potable water to clients; and 7) price volatility.

3.2 Infrastructure Assets and Asset Management

A defining feature of Rand Water is the size and value of its ***infrastructure assets and the dependency*** of Rand Water on the performance of these infrastructure assets.

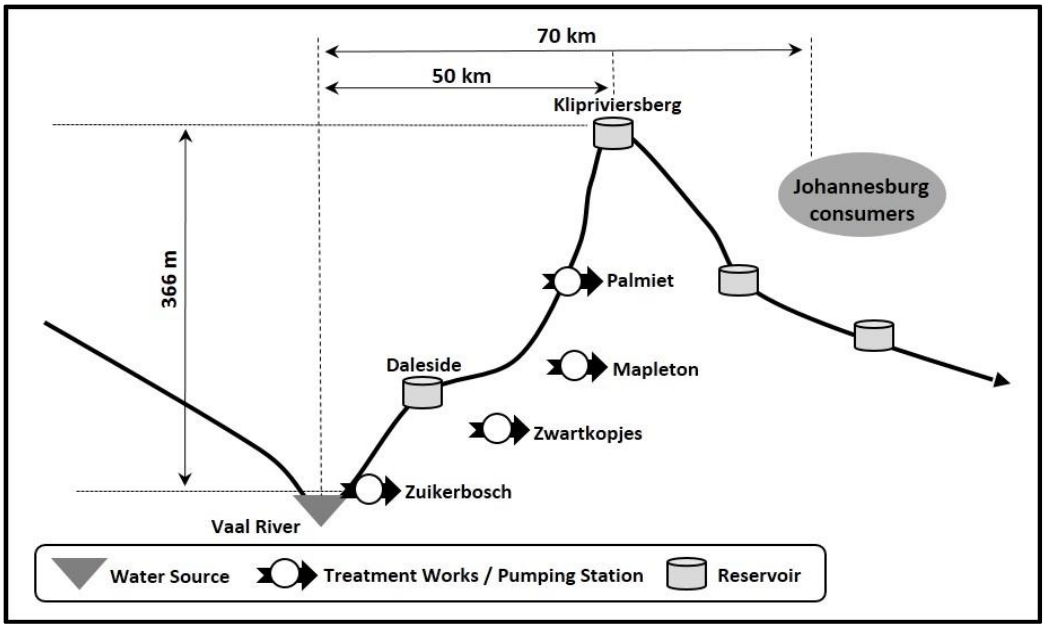


Figure 3-5 Rand Water Source to Consumer (Rand Water, 2003)

The source of water is 70 kilometer (44 miles) away from the bulk of the consumers and the water must be lifted 366 meters from source to destination *(Rand Water, 2003).* As at June 2014, Rand Water operates: 1) a network of 3,500 km (2,188 miles) of pipelines; 2) two large water treatment works next to the Vaal River system; 3) four main booster pumping stations, 4) thirteen tertiary pumping stations; 5) 56 enclosed reservoirs; and 6) numerous secondary booster stations. The largest pipelines are 3 meters in diameter and are situated up to 10 meters underground. The replacement value of the infrastructure assets is ZAR 80-billion *(Rand Water, 2014).*

Rand Water's infrastructure asset portfolio is ***aging*** when compared to the expected useful life of the property, plant and equipment asset classes.

Asset Class	Estimated Useful Life (Years)
Buildings	50 - 80
Plant structures	10
Reservoirs	80
Pipelines	25 - 75

Table 3-2 Infrastructure Asset Useful Life

Some of Rand Water's pipelines are 70 years of age and the majority of pipelines are between 15 and 50 years old. Some components or sections of the pipelines were installed in the 1920's and 1930's. Less than 10% the pipeline network consists of concrete pipes. The rest of the pipes are manufactured from steel. Concrete is more likely to rupture and cause potential damage to people and property. Some pipelines contain small diameter asbestos cement pipes. The concrete and asbestos cement pipelines were identified as high-risk pipelines. A programme to refurbish, renovate and replace pipelines is essential, in order to mitigate the risks associated with the older pipelines.

A ***20-year plan*** is in place that is driven by forecasts of future water consumer needs and the need to maintain the capacity of the existing infrastructure. Rand Water is ensuring that it is ready for the demands of 2030, by focusing on infrastructure renewal and development. Rand Water invested ZAR 2.5 billion in the 2014/15 financial year as part of its ***capital expenditure*** programme. The programme consists of approximately 300 projects.

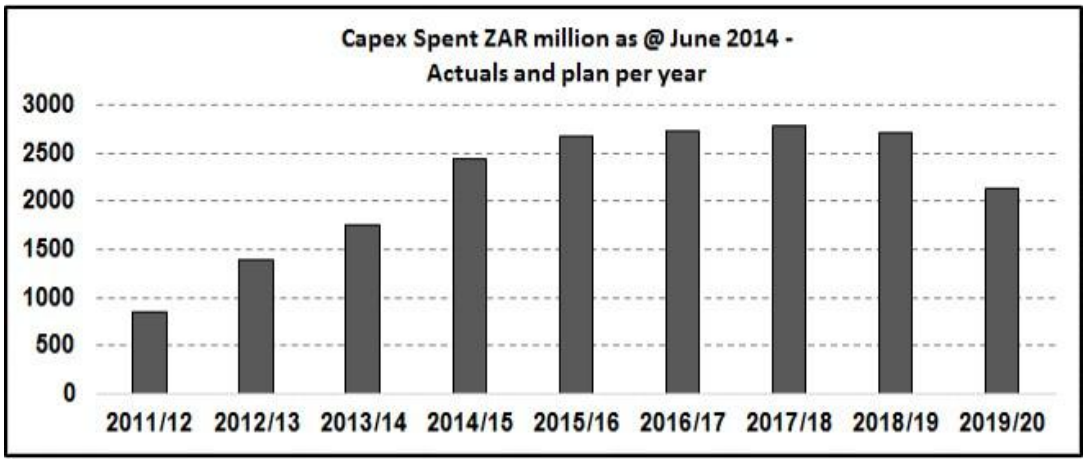


Figure 3-6 Rand Water Capital Expenditure – Actual and Plan (Rand Water, 2014)

Rand Water plans to spend ZAR 13 billion on its infrastructure between 2015 and 2019. Sixty percent of this amount is allocated to infrastructure augmentation projects, with the remaining 40% allocated to infrastructure renewal projects. An additional ZAR 6.8 billion is planned for the same period for growth related projects outside the core business of Rand Water *(Rand Water, 2014).*

The ***management of infrastructure assets*** is a key success factor of the organisation in the achievement of agreed service levels to customers *(Rand Water, 2013).* A range of asset management related methods have been employed to: 1) protect the infrastructure assets; 2) assess the condition and performance of the assets; and 3) prioritise and plan for the required maintenance, refurbishment or replacement of the assets. A comprehensive asset register exists, which is broken down in terms of an agreed hierarchy of assets. It contains sufficient detail to allow proper asset life cycle planning. Standards for design, specification, assessment and maintenance of assets are in place *(Rand Water, 2014).* Some of the key asset management techniques and related technology applied at Rand Water are:

Asset Management Techniques and Technology	Description
Asset condition and performance assessment	A combination of 25 asset condition assessment techniques and technologies are used. This includes aerial surveys using thermal remote sensing, ground penetrating radar, closed circuit television, eddy current analysis, electromagnetic and radio frequency line locators, magnetic flux leak detection, and ultra sound probes.
Asset risk-rating and risk-based prioritisation	Infrastructure assets are ranked in terms of its level of risk, including factors such as age, materials of construction, joint type, and dolomitic ground conditions. Inspections and assessments are performed for the highest risk assets. This feeds into investment planning and prioritisation.

Asset Management Techniques and Technology	Description
Cathodic protection	The Rand Water pipeline network is exposed to corrosion from corrosive soils and microbiological corrosion. This results in metal loss and threatens the integrity of the pipeline network. A cathodic protection system is in place as a corrosion mitigation measure.
Environmental rehabilitation	Environmental rehabilitation of the construction sites ensures that Rand Water's infrastructure is protected from the effects of erosion and other environmental impacts. Eroded land above and adjacent to Rand Water properties, reservoirs and pipelines are monitored, maintained and reinstated.

Table 3-3 Pipeline Asset Management Methods and Techniques (Rand Water, 2013 & 2014)

Rand Water initiated an enterprise-wide infrastructure asset management program in 2012. It adopted the Publicly Available Specification for Asset Management (PAS 55) in 2012 and the ISO 55000 series of standards in 2014 *(Lange & Kasan, 2014; Rand Water, 2014).* An asset management policy, strategy and set of objectives were developed and approved in 2013. A governance structure for asset management was implemented in 2013, including a multi-disciplinary asset management committee, as a sub-committee of Rand Water's executive management committee. The maturity of the asset management practices at Rand Water were assessed by an independent assessor in November 2012 using PAS 55, and again in June 2014 using the ISO 55000 series of standards. The assessment results per KPA were as follows:

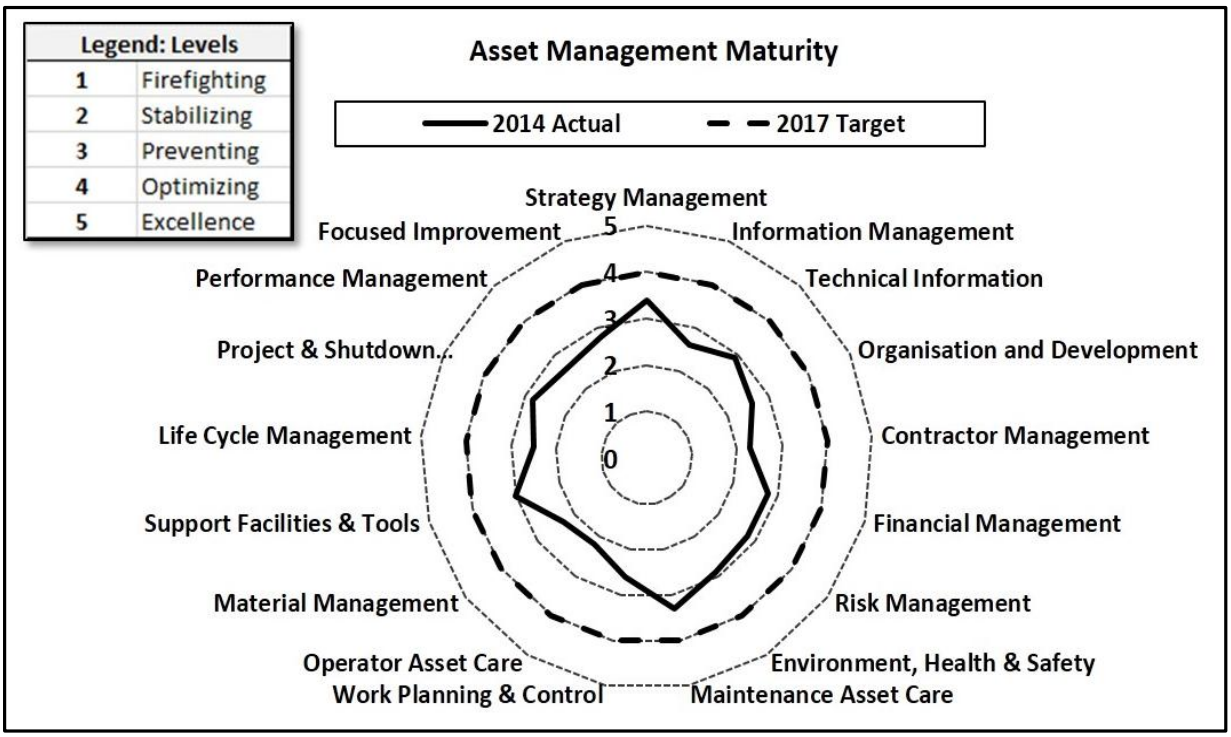


Figure 3-7 Rand Water Asset Management Maturity Assessment Results

The assessments were done using 17 asset management key performance areas (KPAs) and a five level maturity model. The overall rating in 2014 was 2.8, which is between the stabilising and preventing maturity levels of the model. An improvement plan for infrastructure asset management practices at Rand Water was defined, based on the maturity assessment results and Rand Water's target maturity level. It is Rand Water's goal to achieve a level 4 (Optimising) rating for all KPAs and ISO 55000 accreditation by 2017 *(Rand Water, 2014*). The current asset management environment and improvement program provide the basis for establishing a more comprehensive and sophisticated infrastructure asset management approach for Rand Water. This includes the information management KPA, which focuses on the information requirements for asset management and asset related decision making, as well as the supporting digital technology.

3.3 Digital Technology

Rand Water's ***digitisation journey started*** in 1987. A project to computerise the financial processes was approved in 1987. This included a mainframe-based system and a data network *(Rand Water, 2003).* Rand Water had a very conservative view in terms of implementing new or unproven technology that could jeopardise the reliable supply of water in any way. It was reluctant to automate its infrastructure until the early 1990's *(Rand Water, 2003).* The implementation of programmable logic controllers (PLCs) and a supervisory control and data acquisition (SCADA) system was approved in 1992 *(Rand Water, 2003).* This was the start of the digitisation journey for the core business of Rand Water. The digitisation journey subsequently delivered a geographical information system (GIS), geographical positioning systems (GPS), computerised maintenance management system (CMMS), laboratory information system (LIMS), weir management system, a number of decision support systems (DSS), an electronic mail system, PC-based office productivity software and engineering design software products, as well as client-server-based bespoke software systems for Rand Water-specific requirements *(Rand Water, 2003).* Phase one of a three-phase programme to implement an enterprise resource planning (ERP) solution went live in 2005.

The ***Rand Water IT environment, as at 2007***, is the digital technology base case for the research. It represents the start of the change journey. The situation at the time can best be described as an environment in transition. It included a partially completed ERP implementation, as well as numerous other bespoke IT systems and standalone software packages. The ERP implementation was put on hold due to the less than satisfactory results of

the first phase. The informal IT management strategy was a combination of centralisation and decentralisation, but was not applied consistently. There were many digital technology environments that existed due to historical reasons, or events, rather than by design. The ***digital technology organisation*** within Rand Water at that time was segregated. There were three recognised digital technology functions in Rand Water.

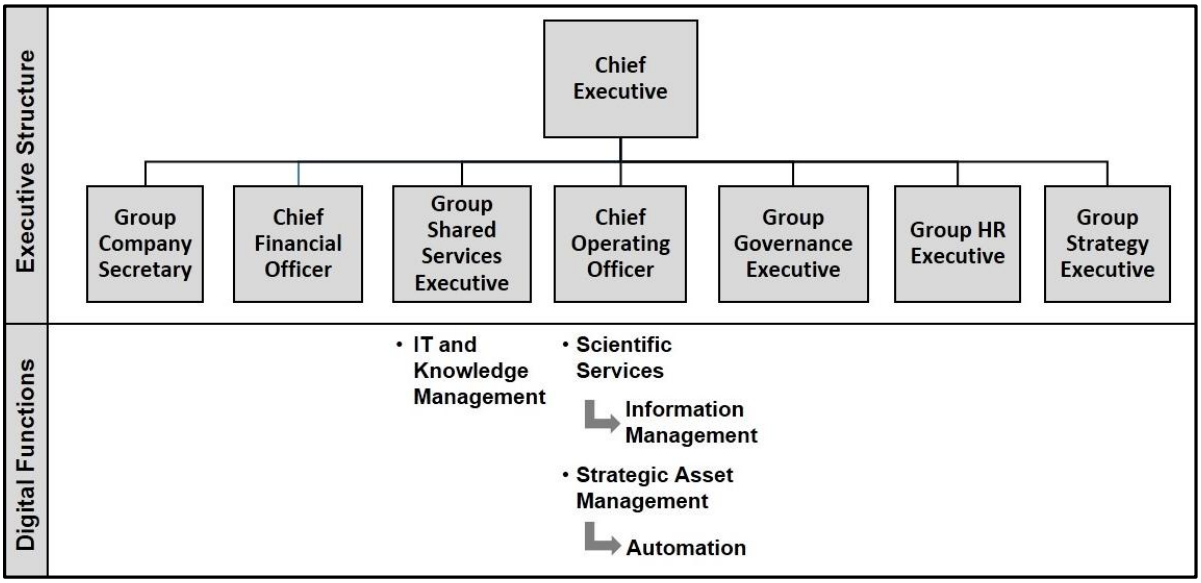


Figure 3-8 Rand Water Digital Technology Organisation

These digital functions were the Information Technology and Knowledge Management (IT&KM) division, the Automation division and the Scientific Services Information Management division. The digital functions were situated within two of the executive portfolios of the organisation, namely the Group Shared Services Portfolio and the Chief Operating Officer Portfolio. The IT&KM function was considered to be the corporate IT function. It was responsible for the majority of the IT solutions. This included enterprise IT systems (e.g. ERP, decision support systems), some business unit-specific systems (bespoke systems and software packages), the wide area data network, some local area data networks, the corporate IT data centre, IT server rooms at the operational sites, the majority of end-user devices (e.g. personal computers and printers), an office productivity software suite (e.g. e-mail) and some of the desktop software. The Automation function is responsible for the SCADA system, telemetry / control networks, SCADA servers and the related instrumentation that support the core operations of Rand Water. It further provided a second level support service to supplement the primary first level SCADA maintenance function within the Operations division.

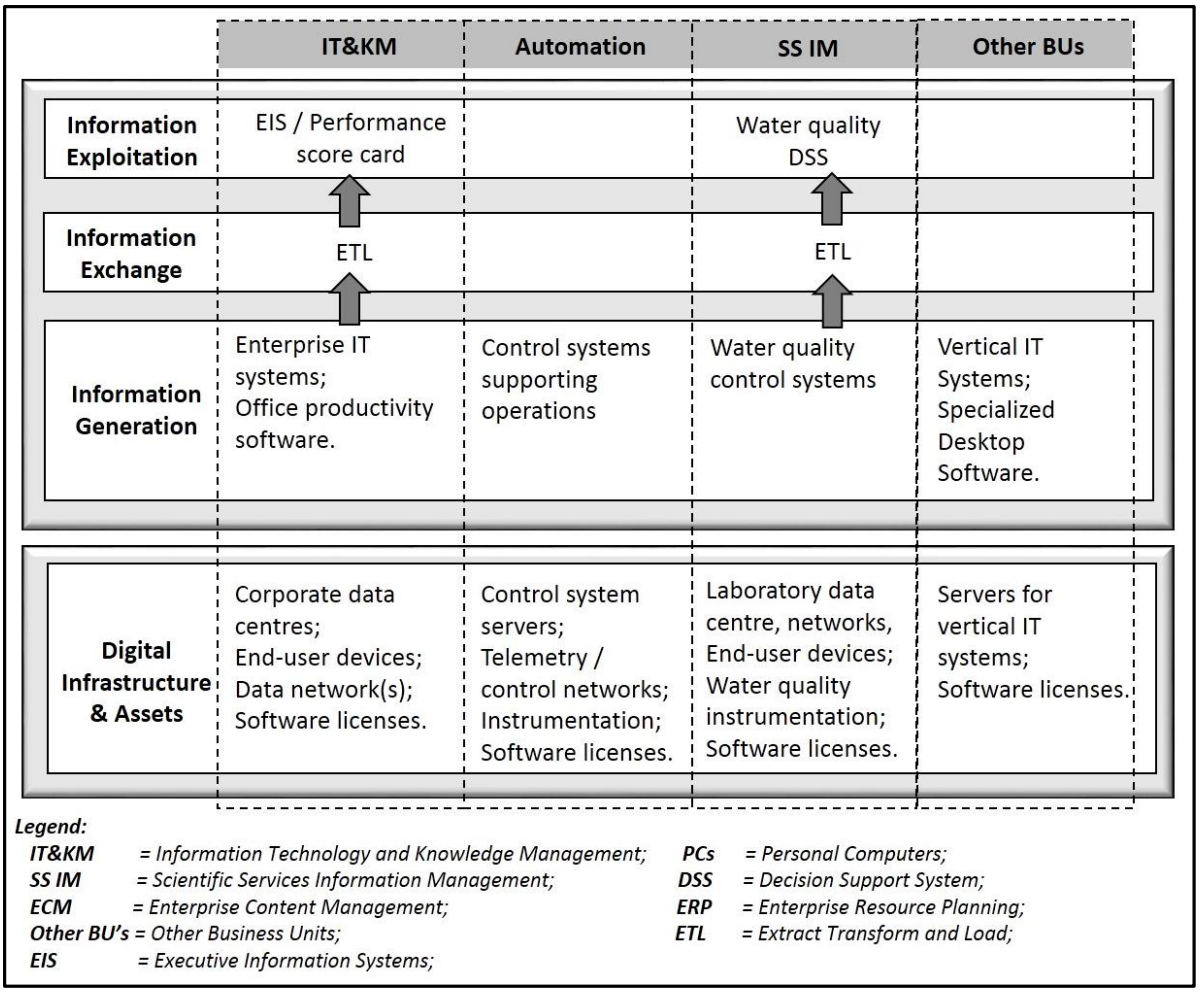


Figure 3-9 Rand Water Digital Technology Solutions Management Responsibility

The Scientific Services Information Management (SS IM) function delivered and maintained water quality and laboratory related control systems (e.g. LIMS, Weir management), water quality decision support IT systems, a dedicated data centre, their local area network, their end user devices, and control system instrumentation supporting water quality monitoring. There were also a number of business units that managed their own vertical IT systems, the related IT servers, and numerous specialised desktop software products. The ***skill sets*** of the three digital functions focused on the solutions that they were responsible for. Although it was different for each digital function, there was some duplication. For example, the Automation function focused primarily on the SCADA and PLC-specific technology and skills, but it also required general server engineering and administration skills. ***Collaboration and communication*** between the digital functions was very limited. The IT&KM division was approached when the other digital functions or business units, who managed their own vertical IT systems, required digital infrastructure components or services for their digital solutions. The ***acquisition and implementation*** of digital products and services was mostly decentralised,

but was coordinated via the corporate procurement function. The unofficial IT service management philosophy at the time was "help them to help themselves". The Rand Water ***digital systems landscape*** consisted of 32 systems, namely:

Category	Digital System	Short Name
Enterprise Systems	Enterprise resource planning system	ERP
	Rand Water website	Website
	Executive information system	Exec IS
	Document management system	Doc Man
Vertical IT Systems - Bespoke Software (Oracle)	Water billing system	Billing
	Operational statistics system	Op-Stats
	Water statistics system	W-Stats
	Time-of-use system	Time-o-Use
	Configuration management system	Config Man
	Conference room booking system	Conf Book
	Barcoding system for records files	Barcoding
	File number generating system	Num Gen
	Treasury management system	Treasury
	Loans system	Loans
Vertical IT Systems – Software Packages	Plant maintenance system	CMMS
	File tracking system	File Track
	Pastel accounting system	Pastel
	Medical aid system	Med Aid
	Provident fund system	Prov Fund
	WebAnswer (HR) system	HR Sys
	Risk management system	Risk Man
	Quality management documentation system	Quality Man
	Water quality decision support system	WQ DSS
	Customer relationship management system	CRM
	Geographical information system	GIS
Control Systems	Supervisory control and data acquisition system	SCADA
	Laboratory information management system	LIMS
	Weir management system	Weir Man
	Global positioning system	GPS
	Automated meter reading	AMR
	Reservoir telemetry system	RTS
	Consumer flow meter telemetry system	CFMTS

Table 3-4 Rand Water Digital Systems Inventory

Each digital function had its own digital landscape design, but no enterprise-wide architecture existed. There was limited integration between the IT systems. The integration of LIMS data into the water quality decision support system was the only example of integration between IT and control systems. No integration between the other control systems and IT systems existed to support asset management decision making. There was also some degree of duplication in

the digital systems landscape in terms of system functionality and data. The business ownership and management responsibility for each of the IT systems, as at 2007, were as follows:

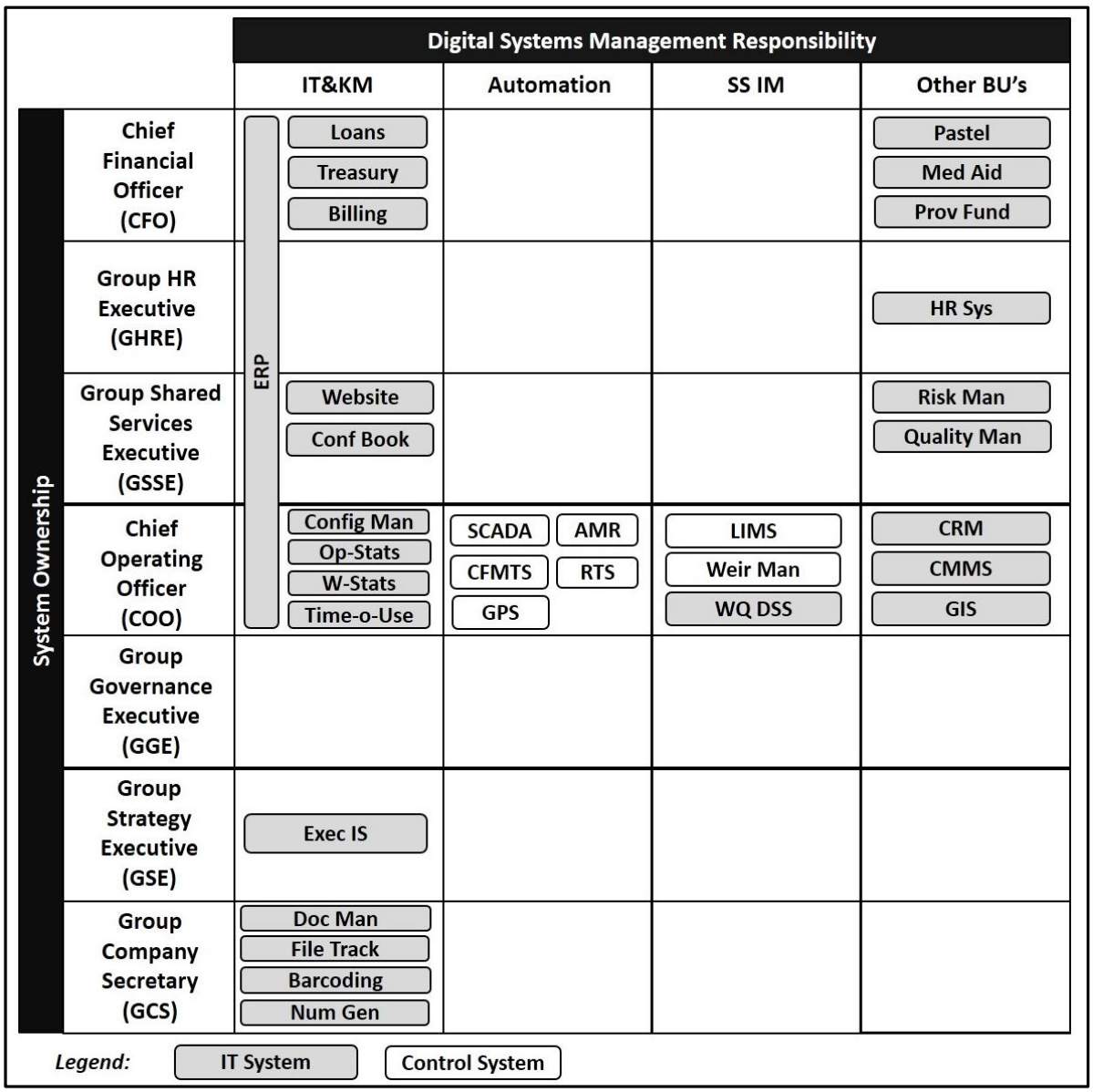


Figure 3-10 Rand Water Digital Systems Ownership and Responsibility

Although there was some degree of convergence in ***digital infrastructure technology*** at Rand Water, it was not yet fully exploited by 2007. All digital systems at Rand Water were client-server-based systems. The pre-ERP mainframe-based financial system was decommissioned when phase 1 of the ERP system went live in 2005. Each digital function had a set of minimum standards that were applicable to their respective digital solutions, including network, software and hardware standards. The level of formalisation of these standards was different for each of the digital functions.

The following are some examples of these standards:

Digital Function	Digital Technology Products and Standards	
IT &KM	Database Management System	Oracle
	Server and PC Operating System	Microsoft
	Data Network	Fibre, Ethernet, TCP IP & Cisco devices
	Servers	Hewlett Packard
	Personal Computers & Printers	Hewlett Packard
	Data Storage	Hewlett Packard
	Data Backup	Arc Serve
	Office Productivity Software	Microsoft
	Enterprise Resource Planning	SAP
	Bespoke Software Development	Oracle Forms & Reports
Scientific Services Information Management	Database Management System	SQL-Server
	Business Intelligence	Crystal Reports
	LIMS	Labware
	Weir – Data Collectors	NMEA protocol, Modbus and Profibus.
Automation	SCADA system	Wonderware
	Database Management System	Industrial SQL Server
	Telemetry Network Devices	Moxa
	Programmable Logic Controller	Gould / Modicon
	Telemetry Network Protocol	Industrial Ethernet & TCP IP

Table 3-5 Examples of Rand Water Key Digital Technology Standards

The IT systems managed by the IT&KM division were hosted within one corporate IT data centre. Those IT systems managed by the business units themselves were mostly hosted in the offices of the respective business units. The decentralised SCADA system installations were hosted in various operations control rooms at plant level. The Scientific Services water quality systems were hosted in a separate dedicated data centre that was located close to the laboratories. All major Rand Water operations sites had: 1) an IT server room, where all IT servers, data storage units and core switches were hosted for that site; 2) an operations control room for the operations staff and the SCADA system; and 3) a telecommunications room for the private automatic branch exchange (PABX) and the connection to the public switch network. There were three distinct networks at each site, namely a dedicated voice network, a corporate IT / data local area network and a control (telemetry) network.

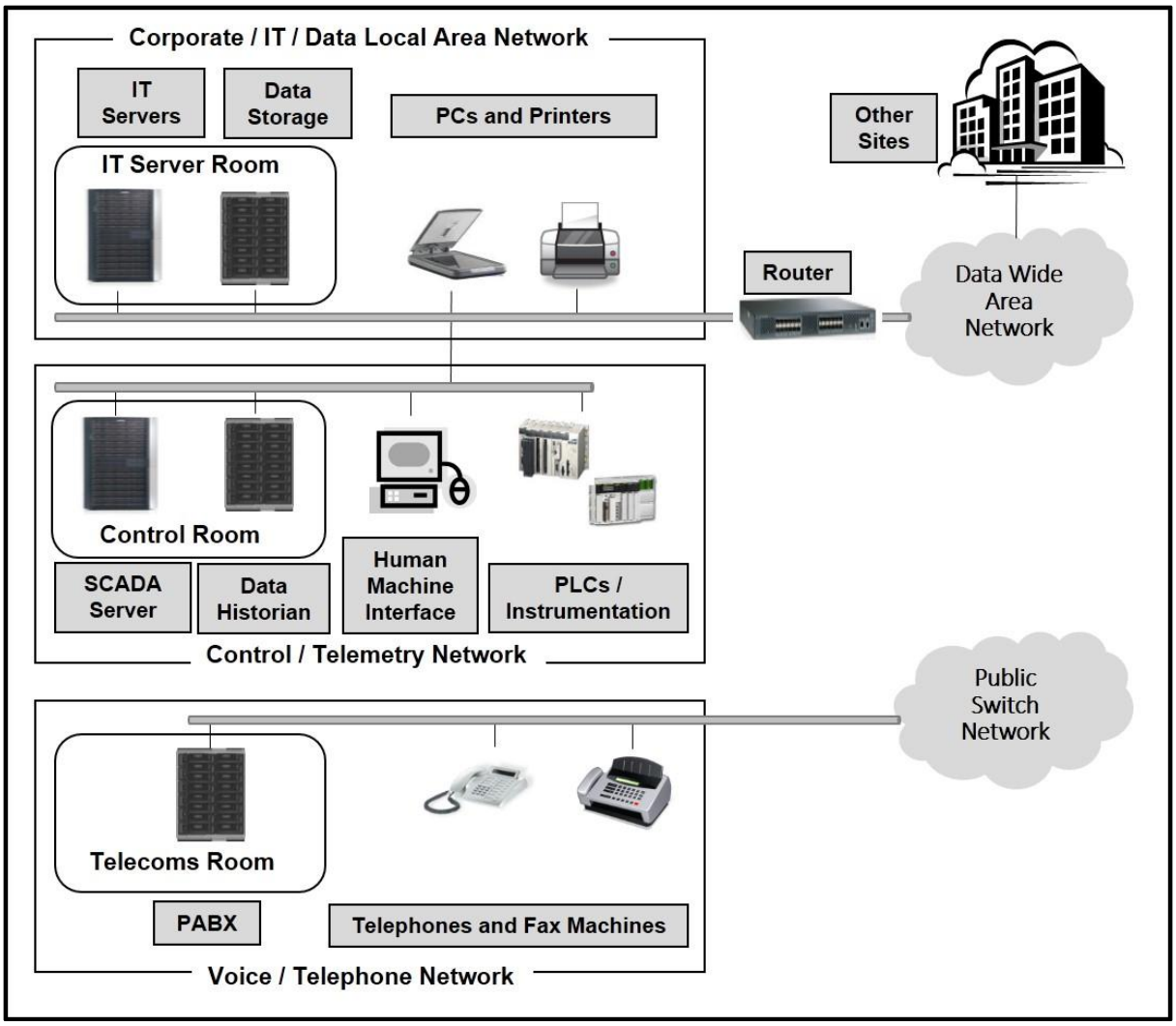


Figure 3-11 Rand Water Operational Site Network Design

The voice network was used for analogue telephony only. It connected the PABX, the public switch network and all the phones and fax machines at the site. All IT equipment, including servers, data storage devices, personal computers (PCs) and printers, were linked to the IT / corporate data network at the site. All the SCADA equipment, including the control server, data historian, human machine interface (HMI) component and the Programmable Logical Controllers (PLCs), were generally linked to the control network at the site. However, this was not consistently applied. There were cases where some SCADA equipment were linked to the IT data network. In such cases, a connection between the control network and the IT network existed, but without any security measures between the two networks. The network design for the Rand Water operational sites was not consistently applied or formally agreed between the Automation and IT&KM functions. A different design was applicable to the digital environment supporting the water quality laboratories. The digital infrastructure fully exploited the convergence in digital technology. All control systems, IT systems, control system

instrumentation, servers, and end-user IT equipment in that location were connected to a single converged data network. The servers were hosted in a laboratory-specific data centre. The risks of full convergence was deemed acceptable for this environment, because the water quality laboratories do not directly impact the 24x7 plant availability of operations. The telephony network was a separate dedicated analogue voice network.

Below are some ***additional and relevant key characteristics*** of the Rand Water digital environment, as at 2014, that provide an indication of the nature and size of the Rand Water digital environment:

Description	Value	Notes
Annual digital operational expenditure	ZAR 150 million	
Annual capital budget	ZAR 150 million	For capital projects and the acquisition of movable digital assets.
Number of users	2,000	Approximately 50% of total Rand Water permanent staff complement.
Number of Rand Water sites supported	30	Includes 6 primary sites, where 90% of users are situated, and 22 satellite / smaller sites spread across the Rand Water area of service.
Number of data centres, server rooms and control rooms.	10	Includes the two data centres, site-specific server rooms, and site-specific control rooms.
Number of movable digital assets	7,000	Includes IT and control system related servers, PCs, printers, instruments and network devices.
Number of software licenses managed	17,000	Includes digital systems / applications and desktop software products.
Number of security incidents per year	20,000	Number of external unauthorised access and malicious software attacks on average per year.
Number of wide area network lines	40	Permanent wide area network links, including links to external entities.
Amount of digital data stored and managed	100 Terabyte	Includes IT and control system data, as well as structured and unstructured data.
Number of servers managed	350	Includes physical and virtual servers enabling IT and control systems.
Number of staff in digital functions	100	Permanent staff members, excluding contractors or temporary project members.

Table 3-6 Additional Key Rand Water Digital Technology Characteristics

Digital governance was catered for by the Rand Water corporate governance framework, including the corporate governance structures and the corporate delegation of authority matrix. This matrix defined the decision making authority for committees and individual positions, such as the approval of capital investments and the acquisition of goods and services. It included IT and, where necessary, specified IT-specific decisions (e.g. capital investment decisions for IT). IT governance was generally not defined separately from the rest of the organisation or extensively addressed by the generic corporate governance framework. There were no IT-specific governance framework, structures or processes. An IT steering committee was established in 2007. It included IT, control system functions and business unit representation, but it only focused on IT services and architectures. Risk management was one of the key components of the corporate governance framework that also covered digital related risk management. An IT operational risk register existed and there was one IT related risk on the organisation's corporate risk register. There were some ***operational controls*** in place to mitigate the typical and most common digital related operational risks, such as access and identify management (e.g. physical access to data centres, user account management, firewalls), as well as the backup and recovery of some of the digital systems and data. There was no formal IT controls framework and the controls were not at the same level of maturity for all the digital functions.

Chapter 4 - Compilation of the Requirements

The purpose of this chapter is to compile the requirements of the artefact by identifying and describing the problems that must be resolved by the artefact. This will be achieved by abstracting the relevant problems from the base case and supplementing it from literature in order to generalise the problems. The generalised problems will be identified and described in terms of technology, process and people related dimensions.

4.1. Problem Dimensions

The overall problem includes the inability to integrate digital technology, information, processes and people, as well as the lack of understanding of how to implement it in an organisation *(Soloman, 2010).* Successful re-engineering initiatives should at least address the organisation, business processes, information flows and the use of information technology *(Manganelli & Klein, 1994).* One of the principles of IT governance is to address the problem in a holistic manner, including people, information, technology and process related dimensions *(IT Governance Institute, 2012).* The problems will be discussed in terms of the following dimensions: 1) technology and information; 2) process; and 3) people.

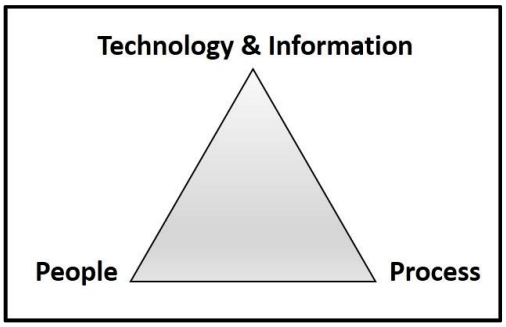
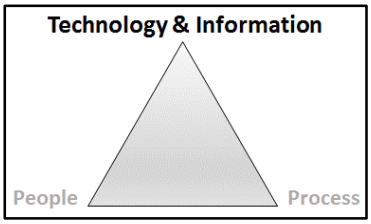


Figure 4-1 Problem Dimensions

The technology dimension includes the exploration of the digital technology related problems, as well as those problems related to the asset information that is processed, stored, communicated and utilised via the digital technology. The process dimension includes the relevant digital governance and operational process control related problems. The people dimension includes organisation and culture related problems. These dimensions are not mutually exclusive and influence each other.

4.2. Technology and Information Problems



The purpose of this section is to describe the generalised technology and information related problems. It includes technology and data size and complexity related problems, as well as problems related to the lack of technology and information compatibility and integration.

4.2.1. Technology size, complexity and increasing sophistication

An asset information related digital systems landscape ***can be extremely large, complex and heterogeneous*** in nature *(ISO, 2014; Soloman, 2010).* The digital environment of an asset intensive organisation consists of a variety of digital systems, media and technology *(Soloman, 2010; ISO, 2014).* Each of these satisfies different business needs and utilises different technical architectures *(Soloman, 2010).* In nearly a decade, operator interfaces evolved from simple panel displays to complex human–machine interface digital technology using thin clients, handheld computers and cell phones *(The Water Environment Federation, 2007; Fernández-de-Alba, Fuentes-Fernández & Pavón, 2013).* Control systems also became larger and highly distributed by using wireless communications networks, such as radio and cellphone networks *(Wang & Shuo, 2013; The Water Environment Federation, 2007).*

The ***sophistication*** of the digital technology and information landscape of infrastructure asset intensive organisations is ***ever-increasing*** due to: 1) more advanced "smart" digital instrumentation; and 2) improved financial feasibility of adopting more sophisticated control systems *(Global Water Intelligence, 2013; Hammoudech & Newman, 2013).* The wider adoption of more sophisticated control systems is becoming financially feasible, due to the reduction in control system cost versus the increased value that it offers the organisation *(The Water Environment Federation, 2010; Hammoudech & Newman, 2013).* Examples of the advancing level of sophistication and intelligence of instrumentation include: 1) "smart" grids for power utilities; 2) "smart" devices for computer-integrated manufacturing; and 3) "smart" networks for water utilities *(Fernández-de-Alba, Fuentes-Fernández & Pavón, 2013; Global Water Intelligence, 2013; Rice & Almajali, 2014).* The adoption of such technologies in the water sector is already in progress and will be more widely adopted by 2018 to manage customer metering, non-revenue water, operational efficiency and water quality *(Global Water Intelligence, 2013).* Advanced meter infrastructure networks are deployed worldwide in the

energy sector, with a penetration of 30% in the United States in 2012 *(Federal Energy Regulatory Commission, 2013).*

The increasing size, sophistication and complexity of digital technology can be a significant problem. This includes all four dimensions of complexity, namely: variety, heterogeneity, dynamics and lack of transparency *(Kluth, Jäger, Schatz & Baurenhansl, 2014).* The ***lack of agility*** of the digital architecture is one of the top ten concerns of IT functions *(ISACA, 2012).* It prevents the timeous response of digital functions and landscapes to changes in the organisation, including: 1) additional digital systems and data sources; 2) organisational growth; and 3) changes to organisational structure and processes *(Iyamu, 2011; Šaša & Krisper, 2011).* The increase in size, complexity and sophistication of control systems reduces the agility of the digital architecture. This creates problems related to the management of changes to the enterprise's digital landscape *(Zachman, 2003).* The digitisation of control systems, the convergence in technology and the increase in control system size and complexity create information ***security related problems*** for the control system landscape (e.g. malicious software attacks) *(Macaulay & Singer, 2012).*

4.2.2. Interoperability and data exchange

Control systems are often standalone and isolated from other information systems *(Macaulay & Singer, 2012; ISO, 2014).* One of the reasons for the isolation of IT and control system networks is the reduction in information security risk of control systems linked to critical installations *(The Water Environment Federation, 2007).* Control systems can provide a wealth of valuable information for decision making, but the data is not useful if it cannot produce proper reporting information or allow the data to be accessible and usable *(The Water Environment Federation, 2010).*

Ensuring ***interoperability,*** namely the ability to share information and services, is a key technology architecture problem in a large complex environment *(Šaša & Krisper, 2011; Zandi & Tavana, 2012).* The implementation of a new control system often creates an interoperability, or compatibility, problem *(Soloman, 2010).* This is due to: 1) the use of proprietary technology; 2) the lack of industry standards; and 3) the cost associated with re-investing in compatible technology *(The Water Environment Federation, 2007).* Two of the reasons for utilising proprietary technology for control systems are: 1) to improve the performance of specialised control systems and to overcome the limitations of commercially available IT solutions; and 2) "all-inclusive" control systems that provide all the required

functional capabilities, and therefore do not need to interface with other digital systems *(The Water Environment Federation, 2010).* However, the situation is improving. Organisations are no longer restricted to proprietary control system software due to: 1) the convergence in digital technology; and 2) the utilisation of open protocols and digital industry standards *(The Water Environment Federation, 2007).*

4.2.3. Big data

Big data related problems include all four characteristics of "big data", namely volume, variety, velocity and value *(Chang, Kauffman & Kwon, 2014).* There is an abundance of data created by control systems *(von Petersdorff, 2013).* However, there are many issues involved in collecting, verifying and consolidating asset data, in order to transform it into asset information *(ISO, 2014).* The big data related problems are applicable to each of the phases of the knowledge discovery process, from data recording to decision making *(Chen & Zhang, 2014).*

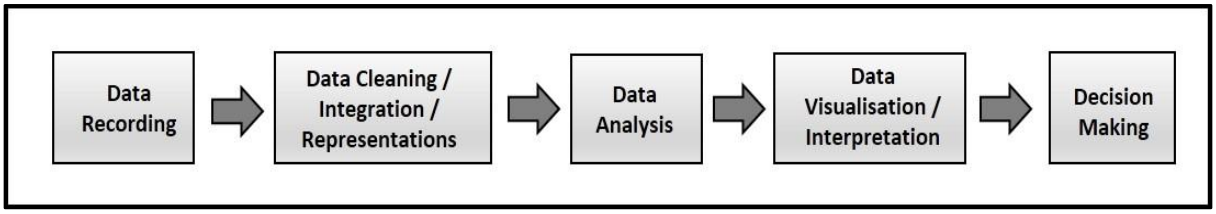


Figure 4-2 Knowledge Discovery Process (Chen & Zhang, 2014)

Data collection and the management of asset data can be costly and the organisation might not have the ability to maintain the appropriate quality and timeliness of the information *(ISO, 2014).* This includes both the consistency and completeness dimensions of data quality *(Kwon, Lee & Shin, 2014).* The quality and quantity of the data used is directly related to the accuracy of the simulation models used for asset decision making *(von Petersdorff, 2013).* However, when making decisions, managers seldom have all the relevant and necessary information required for pure analytical decision making *(Dhami & Thomson, 2012).* Assumptions need to be made in such cases. These assumptions may detract from the usefulness and the level of acceptance of the analysis or simulation results *(von Petersdorff, 2013).* Compliance to data retention related legislation is an additional "big data" related information management problem, in an environment with a high volume and wide variety of asset data *(The Water Environment Federation, 2010).*

The ***volume of the data*** is increasing at an exponential rate and originates from multiple sources, including people and "smart" high-throughput instrumentation (e.g. sensor networks, telescopes, scientific experiments) producing granular data about the environment and

infrastructure assets *(Global Water Intelligence, 2013; Hammoudech & Newman, 2013).* There are 2.5 quintillion bytes of data created every day, and this number keeps increasing exponentially (*Chen & Zhang, 2014).* Big data is a relative term and what constitutes big data changes over time. For example, a NASA Apollo 11 computer in 1969 with a memory of 32 KB versus a single NASA data set in 2013 of 10 Zettabytes *(Douglas, 2014).* It is a significant problem to process, manage and utilise a collection of very large diverse asset data sets by using typical data processing approaches or technology platforms *(Lehman & Heagy, 2014).* It is estimated that as at June 2015 approximately 90% of all the data in the world has been created in the past two years *(Huard, 2015).* The world's technological capacity to store information has doubled every 3 years since the 1980's, but the exponential increase in data size has surpassed the capabilities of computation *(Chen & Zhang, 2014).*

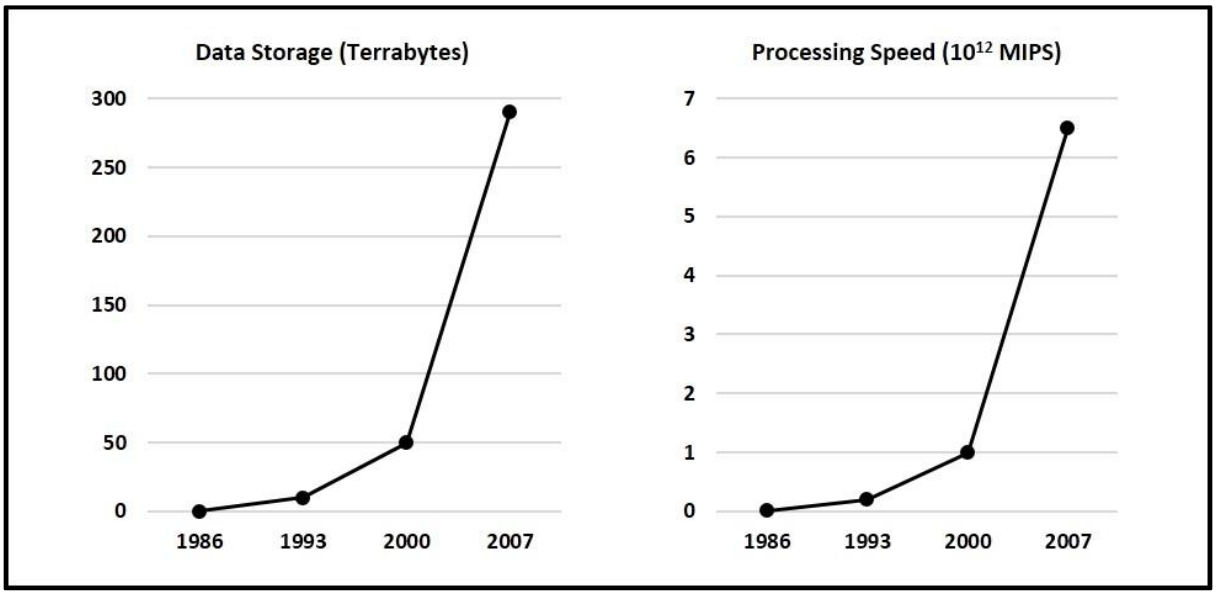


Figure 4-3 Data Size Exceeds Computation Capacity (Chen & Zhang, 2014)

Valuable data, that were created and captured at high cost, is being discarded, because: 1) data is often deleted just because there is not enough space to store it; and 2) the existing database management tools are unable to cater for big data curation, including archiving, management, preservation, retrieval, and representation (*Chen & Zhang, 2014).* Asset condition assessment techniques and technology also contribute to the increase in data volume *(Lau & Dwight, 2011).* This includes unstructured data, from a combination of technologies used to locate and assess underground infrastructure assets *(Costella, Chapman, Rogers & Metje, 2007).*

Asset data is located across diverse digital systems in a ***variety of data*** formats *(Soloman, 2010; ISO, 2014).* Some of the information originates from external sources, such as contractors, key suppliers and customers *(Institute of Asset Management, 2008).* Data formats include

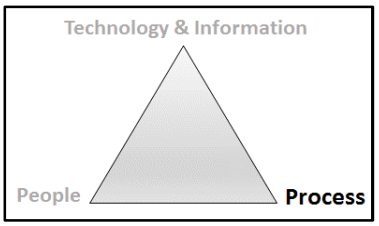
structured data (e.g. enterprise asset management system) and unstructured data (e.g. images, text, videos) using electronic or paper-based media *(Chang, Kauffman & Kwon, 2014; Hammoudech & Newman, 2013).* Asset condition assessment technology also produces a variety of structured and unstructured data *(Costella, Chapman, Rogers & Metje, 2007).* This includes ground penetrating radar, infrared thermography surveys, closed-circuit television, magnetic flux leak detection and ultra sound *(Lau & Dwight, 2011).* It is still a problem to efficiently access, analyse and represent unstructured or semi-structured data ***(****Chen & Zhang, 2014).* The same asset data element is often treated differently by different individual systems due to: 1) inconsistent data definitions (e.g. data definition language, data taxonomy); 2) different technologies; 3) different data types and formats; and 4) a lack of knowledge regarding the relationship amongst data elements stored within different systems *(Leung, Ji & Ma, 2013).* The problem in such a data landscape is to: 1) share the data between systems; and 2) communicate and present a wide variety of information from a wide variety of sources in a consistent and useful way to people *(Soloman, 2010).* Evidence-based multi-stakeholder group decision making requires information from different sources, which can produce conflicting evidence *(Leung, Ji & Ma, 2013).* The lack of data accessibility is partially caused by the lack of the technical capability required to harmonise, consolidate or fuse multi-source information, in order to provide consistent and aggregated evidence required for problem solving *(Fernández-de-Alba, Fuentes-Fernández & Pavón, 2013).*

Operational level decision making for day-to-day tasks (e.g. work scheduling) requires ***high-velocity*** up to date, or real-time, information *(Burns, 2010; von Petersdorff, 2013).* Satisfying high velocity data requirements is a problem for normal IT system integration platforms *(Soloman, 2010).* However, data velocity is not a significant problem for strategic asset decisions. Unlike operational decisions, strategic asset decisions does not require a high data velocity *(von Petersdorff, 2013; Lehman & Heagy, 2014).*

More data does not always ***add value*** and might only yield more confusion *(Woodhouse, 2010).* The data that are critical for an organisation, in order to make the different types of asset decisions (e.g. operational versus strategic), are often counter-intuitive, due to the lack of an asset information strategy *(Edwards, 2010).* The resulting new asset digital system might therefore: 1) be more expensive than what it should be: and 2) not provide the correct data, at the right level of quality, at the right time, to the right people, in order to effectively support their asset activities *(Edwards, 2010).* It is a problem to ensure that only the relevant and useful,

or valuable, information is extracted from a large volume of heterogeneous data, and made available for decision making *(Lehman & Heagy, 2014; Hammoudech & Newman, 2013).*

4.3. Process Problems



The purpose of this section is to describe the generalised process related problems. It includes information security, digital governance and operational process control related problems of the digital environment.

4.3.1. Information security

The ***scope of information security problems*** includes the integrity, availability, and confidentiality of information *(Rice & Almajali, 2014; ISO, 2005).* Availability is the primary security related concern for control systems, due to the impact on plant availability *(Wang & Shuo, 2013).* The integrity of information impacts the integrity of the plant and decision making *(Anwar & Mahmood, 2014).* The confidentiality of information has the least impact on plant availability and integrity, but is an increasing risk for organisations with demand-side management programs *(Campbell, 2011; Wang & Shuo, 2013).* This is due to privacy requirements and the protection required against the misuse of personal and proprietary information (*Anwar & Mahmood, 2014).*

The protection of information resources from the complex and rapidly evolving ***security threats*** is a significant problem in the modern organisation *(Webb, Ahmad, Maynard & Shanks, 2014; Jaatun, Røstum, Peterson & Ugarelli, 2014).* The information assets of an organisation is at constant risk, now more than ever before *(Silva, de Gusmão, Poleto, e Silva, & Costa, 2014).* The number of known cyber security incidents in the electricity sector between 2004 and 2008 increased by 20% from the previous four years *(Anwar & Mahmood, 2014).* "Smart" grid requirements and technologies evolve over time *(Campbell, 2011).* The potential risks associated with control system security increase as the level of automation, the level of sophistication, the number of new devices, and the market penetration of control systems increase *(Federal Energy Regulatory Commission, 2013).* Staying ahead of the ever-increasing security threats will result in a never ending cost for organisations *(Campbell, 2011).* Cyber security spending is estimated to be 15% of the US$ 1.5 billion smart grid capital investment in North America between 2010 and 2015 *(Campbell, 2011).*

The ***convergence of digital technologies and integrating control and IT systems***, in order to share asset data, increases the security risk of operations *(Rice & Almajali, 2014).* It introduces new security vulnerabilities and exposes the physical plants, the control systems and the IT systems to both intended and unintended threats from internal and external to the organisation *(The Water Environment Federation, 2007; Anwar & Mahmood, 2014).*

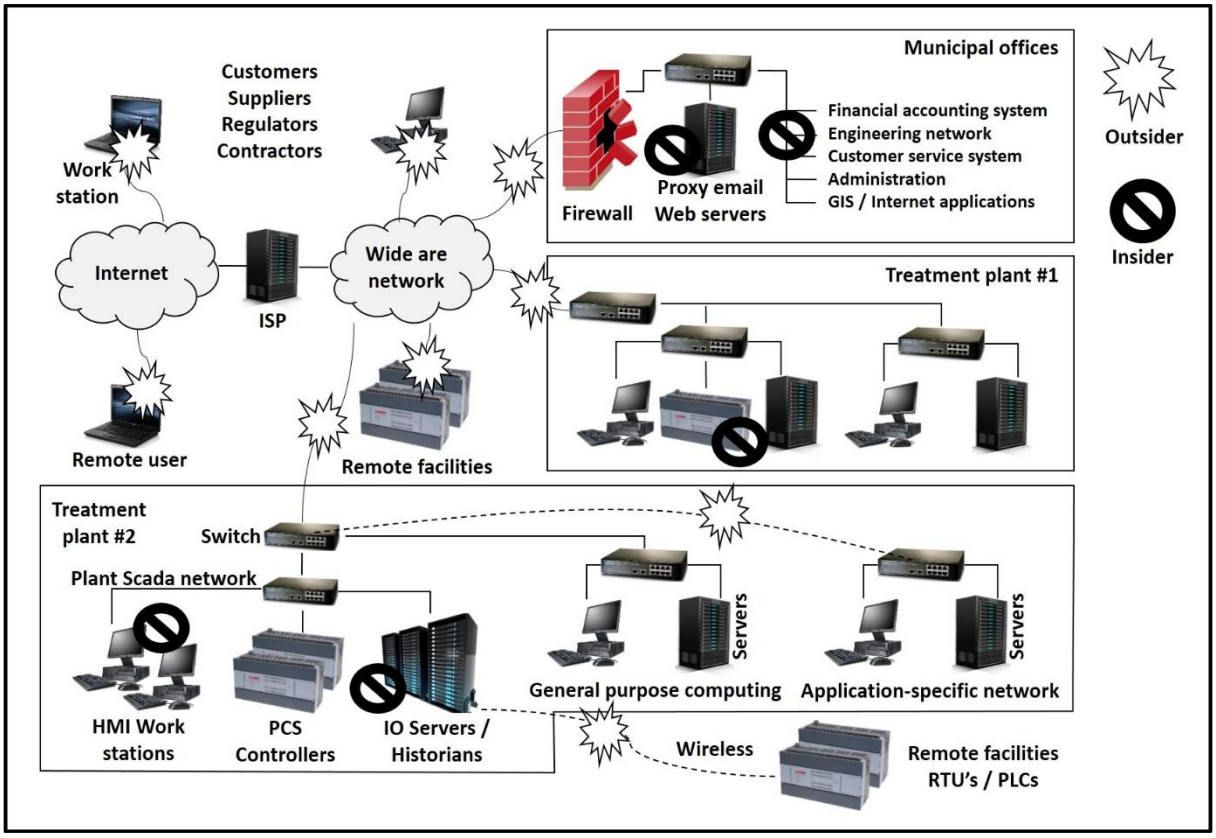


Figure 4-4 Common Control System Cyber Vulnerabilities (adapted from The Water Environment Federation, 2007)

It is important to have adequate information security measures to protect the digital landscape, whilst still satisfying the organisation's accessibility, efficiency and cost saving requirements *(Shariati, Bahman & Shams, 2011).* It is a significant problem to achieve an optimal balance between these conflicting and evolving needs and priorities *(Wang & Shuo, 2013).*

Control systems were originally ***not designed with cyber security in mind.*** Their cyber security measures are therefore often weak *(Campbell, 2011).* Although redundancy and reliability were an integral part of the overall computerised control system architecture and design, cyber security was not a top priority (*The Water Environment Federation, 2007).* It was too costly to include security measures in the control system design (*Macaulay & Singer, 2012).* Legacy control systems and devices were sometimes retrofitted with communication capabilities and

"smart" instrumentation, as a cost effective method of modernising the control system landscape *(Campbell, 2011).* This approach increases the information security risk, as the cyber security weaknesses remain within the retrofitted system that is now part of the interconnected control system landscape *(Campbell, 2011).* Control systems now need to be secured from both physical and cyber threats, ranging from amateur hackers inadvertently damaging a control system, to state-sponsored terrorists intend on mayhem *(The Water Environment Federation, 2010).*

The ***interconnected digital communication network*** has become a critical element of the overall digital infrastructure *(Jaatun, Røstum, Peterson & Ugarelli, 2014).* Control systems traditionally consisted of closed networks with no outside communication, but this is rapidly changing *(Jaatun, Røstum, Peterson & Ugarelli, 2014).* Internet-linked and wireless communication systems, including remote instrumentation (e.g. machine to machine "internet-of-things") and cell phone networks, are now an important part of the connected digital landscape *(Campbell, 2011; Wang & Shuo, 2013).* It is also a key vulnerability for control system security, since it provides an additional path for cyber-attacks from anywhere in the world *(Campbell, 2011).* Remote access to a control system by operator employees is the least protected entry point, or "weakest link", in terms of security *(Jaatun, Røstum, Peterson & Ugarelli, 2014).* In 2011, 35% of control system security incidents were instigated via remote access to a control system *(Anwar & Mahmood 2014).*

The potential ***negative implications*** of the failure of the physical plants, due to cyber security attacks, are far reaching and beyond the impact on information *(Campbell, 2011).* Information security threats are applicable to all industries that utilise control systems and "smart" technology, including the electricity, natural gas, telecommunications, water and manufacturing industries *(Soloman, 2010; Jaatun, Røstum, Peterson & Ugarelli, 2014).* These industries are also dependent on each other and the failure of one can have a cascading affect *(Campbell, 2011).* The impact of cyber security failures include potential loss of revenue, operational disruptions, non-compliance to legislation, lack of investor confidence, reputational damage, social and welfare implications, destruction of critical infrastructure, damage to the economy, national security and loss of human life *(Wang & Shuo, 2013; Rice & Almajali, 2014).* One hour IT downtime can potentially cause a loss in revenue of between US$ 90,000 and US$ 6.48 million, and a reduction in sales of between 28% and 39% *(Benaroch, Chernobai. & Goldstein, 2012).* The 2010 Federal Bureau of Investigation Computer Crime and Security Survey on 738 organisations reported a total estimated annual

loss of US$ 190 million caused by information system security incidents *(Feng, Wang & Li, 2014).* The consequences of control system security failures can have physical and immediate consequences to critical national services, because control systems are usually linked to critical infrastructure (*Macaulay & Singer, 2012).* In one experiment, a "dummy" water treatment plant control system server was made accessible to the internet. It received 39 attacks in one day and several of these attacks attempted to change water pressure or manipulate pumps *(Jaatun, Røstum, Peterson & Ugarelli, 2014).* There are also dedicated search engines specifically attempting to locate industrial control systems connected to the internet *(Jaatun, Røstum, Peterson & Ugarelli, 2014).* "Hacktivism" is now more sophisticated than ever before. It no longer only focuses on social and political protest, but includes politicised attacks, essential service disruption, espionage and cyber warfare *(Caldwell, Maude & Gallego, 2015).* It is now the number 2 form of attack (18% of the attacks), whilst cyber-crime is number one (71% of the attacks) *(Caldwell, Maude & Gallego, 2015).*

There are ***operational cyber security controls*** and practices that provide the assurance that cyber-attacks will be less likely to succeed, or that the impact of a successful attack can be minimised *(Rice & Almajali, 2014).* These operational controls are supported by increased legislation and penalties for cyber-crimes *(Campbell, 2011).* However, a number of simulations and assessments found that: 1) the existing security measures of control systems and the responsible digital functions are not always effective or adequate for large scale distributed control system networks: and 2) some control systems and responsible digital functions do not comply with recommended cyber security standards, architectures, practices or frameworks *(Anwar & Mahmood, 2014).* There are recorded incidents that support these findings, such as: 1) the Stuxnet software worm in 2010 that targeted Siemens control system equipment: 2) the 2006 power outage in Italy and Switzerland caused by human error; and 3) the 2003 power outage in the USA caused by a software program error *(Anwar & Mahmood, 2014).*

Security frameworks, architectures and standards are ***not enforceable and compliance is voluntary*** *(Campbell, 2011).* The result is a significant variance between industries, geographical areas, organisations, and digital functions within an organisation in terms of security maturity and compliance with security related regulations *(Campbell, 2011).* A successful attack on the "weakest" link of either the IT or control system environment may affect the overall integrated digital environment. It may potentially lead to cascading digital security and system failures within the organisation and beyond *(Anwar & Mahmood, 2014).* The lack of adequate and consistent security measures and the lack of a coordinated response

to threats are therefore common operational risks for both the control system and IT system environments *(Campbell, 2011).*

4.3.2. Low and inconsistent digital governance maturity

The IT governance maturity level of the majority of organisations is below level 3 of a 5 level maturity model (i.e. between ad-hoc and defined) and there is a wide distribution across the maturity levels *(IT Governance Institute, 2011)*. This indicates a relatively ***low level of maturity on average and inconsistency*** between organisations in terms of IT governance. Organisations within asset intensive industries (e.g. manufacturing) and the public sector are less likely to implement IT governance than organisations in the administrative intensive industries (e.g. financial services) *(ISACA, 2011).*

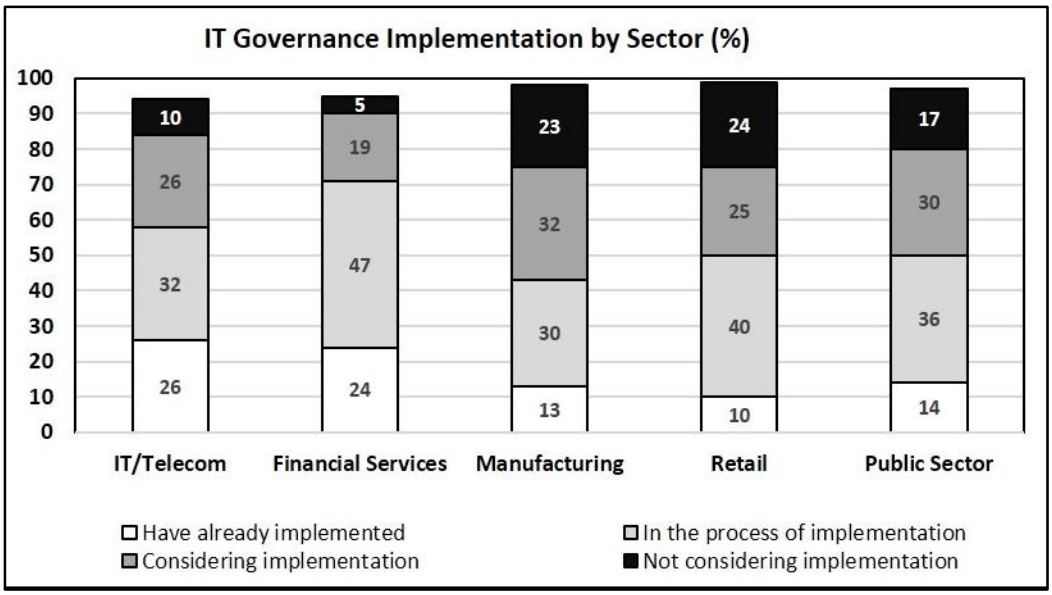


Figure 4-5 IT Governance Implementation by Sector (ISACA, 2011)

According to the ISACA global 2011 survey, only 13% of the participants from the manufacturing sector indicated that they implemented IT governance, whilst 23% indicated that they are not considering implementing IT governance. Only 12% of the total number of participants in the ISACA 2012 survey were from infrastructure asset intensive sectors, such as manufacturing, mining, utilities and transport. Only 3% of the participants were from the utilities sector *(ISACA, 2012).* There is still relatively little guidance for performing risk assessments or evaluating the adequacy of controls and risk mitigating measures for control system environments *(Macaulay & Singer, 2012).* Information security controls and practices in the IT environment are far more mature than in the control system environment (*Macaulay & Singer, 2012).*

4.3.3. Over and under regulation

The lack of balance between over-regulation and under-regulation results in negative side effects for the organisation *(Verhoef, 2007).* Under-regulation results in increased risk and the lack of alignment with business strategy *(Verhoef, 2007).* Over-regulation, or the "perfect control", tends to result in: 1) an increase in cost; 2) a decrease in efficiency and productivity; and 3) a delay in time to market for new IT-enabled products and services of up to 20% *(Verhoef, 2007).* In practice, over–regulation usually results in an overall cost increase without delivering the expected value or reducing risk *(Verhoef, 2007).* This imbalance is especially prevalent in large organisations *(Verhoef, 2007).* It happens for a number of reasons, such as:

Reason	Description
Compliance equals assurance	The organisation: 1) needs to comply with the Sarbanes Oxley Act; or 2) believes that compliance to a standard is adequate assurance *(Matwyshyn, 2009; Kerr & Murthy, 2013; Lunardi, Becker, Maçada & Dolci, 2014).*
Maximum maturity equals assurance	The organisation believes that it should aim at the highest level of IT governance maturity, or complexity, for all the activities, in order to ensure adequate assurance *(Pilling, 2010; Port & Wilf, 2014).*
"One size fits all"	The organisation supports a "one size fits all" approach to IT governance frameworks *(Verhoef, 2007; Institute of Directors of South Africa, 2009).*

Table 4-1 Reasons for Under and Over Regulation

Some organisations treat ***compliance as an end in its own right***, rather than considering the associated risk *(Webb, Ahmad, Maynard & Shanks, 2014).* The regulatory environment and specific compliance requirements is one of the primary factors influencing the implementation of IT governance practices *(Chitambala, 2006; IT Governance Institute, 2011).* Compliance reduces risk by reducing the uncertainty in the quality of the software product, but assurance is more than compliance with standards *(Port & Wilf, 2014).* A pure compliance-based assurance merely assesses compliance with existing procedures and processes, without an evaluation of whether or not the procedure or process is an adequate control *(Institute of Directors of South Africa, 2009).* It is also less effective than a risk-based approach, because it does not allow the assurance provider to determine whether controls are effective in managing the associated risks *(Institute of Directors of South Africa, 2009).* The result is that controls do not go beyond formal compliance and might therefore not be appropriate (*Webb, Ahmad, Maynard & Shanks, 2014; Matwyshyn, 2009).* It is a risk to the organisation to aim purely at compliance with a framework or standard *(Pilling, 2010).*

It is also a risk to the organisation to simply ***aim at the highest level of maturity*** for all activities *(Pilling, 2010).* Especially if this is done without: 1) considering whether the target level of maturity and the recommended best practice are appropriate for the organisation, given the context of the organisation and industry; or 2) tailoring the framework or standard to the organisation's needs *(Pilling, 2010).* The result may be an expensive solution that does not deliver the expected value and does not mitigate the associated risks *(Pilling, 2010).* The cost of assurance can be high and the degree of assurance required in connection with managing risk is not always clear *(Port & Wilf, 2014).* This is a significant problem considering that increased IT cost and insufficient number of IT staff, are two of the highest issues experienced by IT functions (*IT Governance Institute, 2011; ISACA, 2012*).

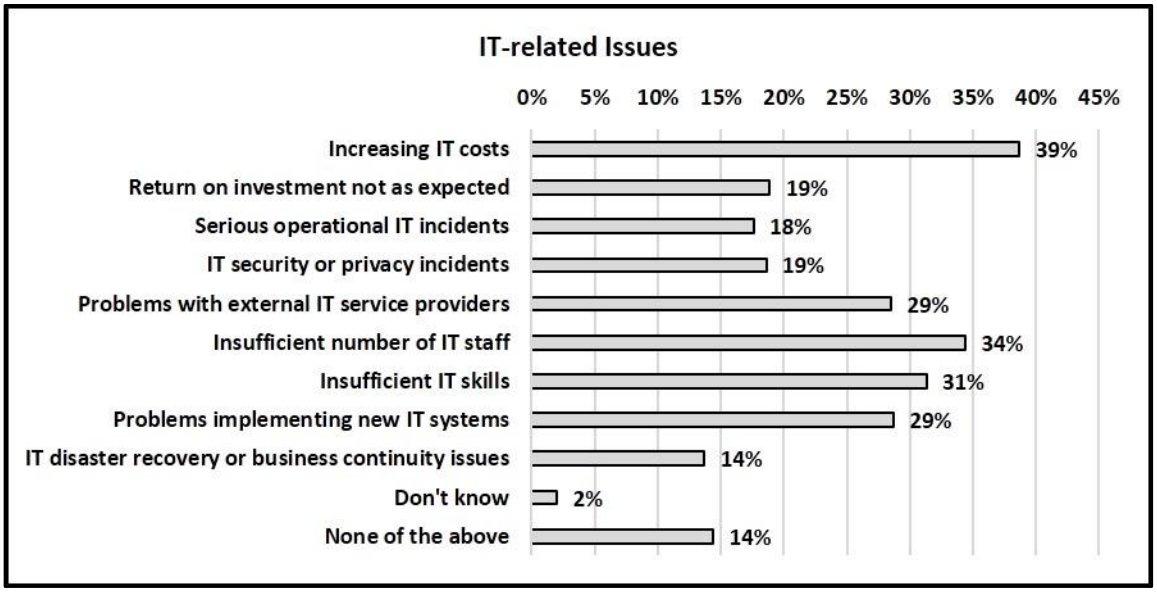
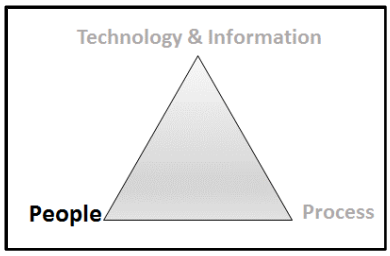


Figure 4-6 IT Issues (IT Governance Institute, 2011)

Complexity is also sometimes confused with maturity. A high level of maturity does not necessarily mean or require a complex expensive solution or process *(Pilling, 2010).*

This is supported by the notion that **"one size fits all"** in terms of IT governance frameworks. Such organisations also believe that: 1) "any structure for IT governance will work as long as senior business executives are involved"; and 2) no deviation is allowed in terms of IT governance and operational controls *(Verhoef, 2007).* A "one size fits all" approach cannot logically be suitable because the types of business carried out by organisations vary to such a large degree *(Verhoef, 2007).* The cost of compliance is also burdensome, measured both in terms of time and direct cost *(Institute of Directors of South Africa, 2009).* An inappropriate approach and level of control, or regulation, causes a lack of balance between risk and value *(Verhoef, 2007).*

4.4. People Problems



The purpose of this section is to describe the generalised people related problems. It includes the organisational and change management related problems of the digital environment of the organisation.

4.4.1. Organisational segregation

Asset intensive organisations, such as utilities, tend to ***segregate the control system and IT system responsibilities*** *(The Water Environment Federation, 2007).* IT functions are generally not made responsible for maintaining control systems or the enabling digital infrastructure *(The Water Environment Federation, 2007).* This segregation can lead to the following problems:

Category	Description
Skills	Insufficient digital skills within the organisation, including the lack of cross-functional skills required for an integrated and converged digital landscape. This includes security skills.
Roles and Responsibilities	Lack of clarity regarding roles, accountability and responsibility of digital systems and activities (e.g. security).
Communication, collaboration and involvement	The lack of communication, sharing of information or knowledge, and collaboration between digital functions, as well as the lack of involvement by digital functions in enterprise-wide digital initiatives.

Table 4-2 Implication of Digital Organisational Segregation

The third highest common issue for IT organisations is ***insufficient IT skills*** *(IT Governance Institute, 2011).* Technical control system personnel are not primarily qualified in information security *(Jaatun, Røstum, Peterson & Ugarelli, 2014).* As a result one might find, for example, that the IT function has an up-to-date firewall for the IT systems infrastructure, but that this is not the case for the control system infrastructure *(The Water Environment Federation, 2007).* The issue is amplified by the lack of, and need for, cross-disciplinary knowledge of the IT and control system functions *(Shedden, Ruighaver, & Ahmad, 2010*). This is especially a problem in some smaller organisations with limited operational resources *(Jaatun, Røstum, Peterson & Ugarelli, 2014).*

There is a ***lack of clarity*** regarding the ***authority, accountability and responsibility*** of the digital functions of the organisation *(Campbell, 2011).* This includes the security related roles and responsibilities (*The Water Environment Federation, 2007).* The implementation of multiple IT governance mechanisms in large, complex, multi business-unit organisations inadvertently creates, or add to, the confusion regarding: 1) decision making authority; 2) accountability for digital solutions; and 3) the responsibility for tasks and processes *(Bowen, Chung & Rohde, 2007).* This confusion can limit the ability of managers to deliver outcomes that they are responsible for *(Bowen, Chung & Rohde, 2007).*

There is a ***lack of collaboration, knowledge sharing and communication*** between the digital functions of the organisations. This can potentially have many negative implications. Some of these will be briefly described. There is generally a lack of collaboration and sharing of information about current and emerging information security threats *(Ahmad, Hadgkiss, & Ruighaver, 2012; Shedden, Scheepers, Smith & Atif, 2011; Colwill, 2009).* This was one of the root causes of the power outages in Italy, Switzerland and the United Stated of America between 2003 and 2006 *(Anwar & Mahmood, 2014).* There is a lack of collaboration and communications regarding IT governance related initiatives *(Prasad, Green & Heales, 2012).* IT governance is kept at a strategic level and is not brought down to the operational level *(Prasad, Green & Heales, 2012).* As such, the operational level is not aligned to the strategic level and IT governance might therefore not have a positive impact on the operational performance of the organisation *(Prasad, Green & Heales, 2012).* The lack of involvement by stakeholders in defining and implementing security practices, is one of the reasons for the lack of security related knowledge of staff *(Flores, Antonsen. & Ekstedt, 2014).* The lack of key stakeholder involvement is also the root cause for enterprise architecture initiative failures *(Fonstadt & Robertson, 2004).* The digital technology incompatibility problem is partially caused by poor communication and the lack of collaboration between the digital functions of the organisation, especially in terms of the selection and acquisition of digital technology *(Soloman, 2010).* The failure of IT strategies and policies can be caused by ineffective communication, regarding the new IT strategies and policies *(Bowen, Chung & Rohde, 2007).*

4.4.2. Resistance to change

It should not be assumed that stakeholders involved in, or impacted by, a new or revised situation will ***readily accept or adopt the change*** *(IT Governance Institute, 2011).* The culture of the organisation, its way of working and human related factors significantly influence the IT

governance practices of the organisation *(ICASA, 2012).* Most of the main problems experienced in implementing IT governance mechanisms are people related problems. These include: 1) resistance to change and the lack of overall change management; and 2) the lack of communication, senior management commitment, business participation, awareness, knowledge and demonstrating value *(IT Governance Institute, 2011; Othman, Chan & Foo, 2011).*

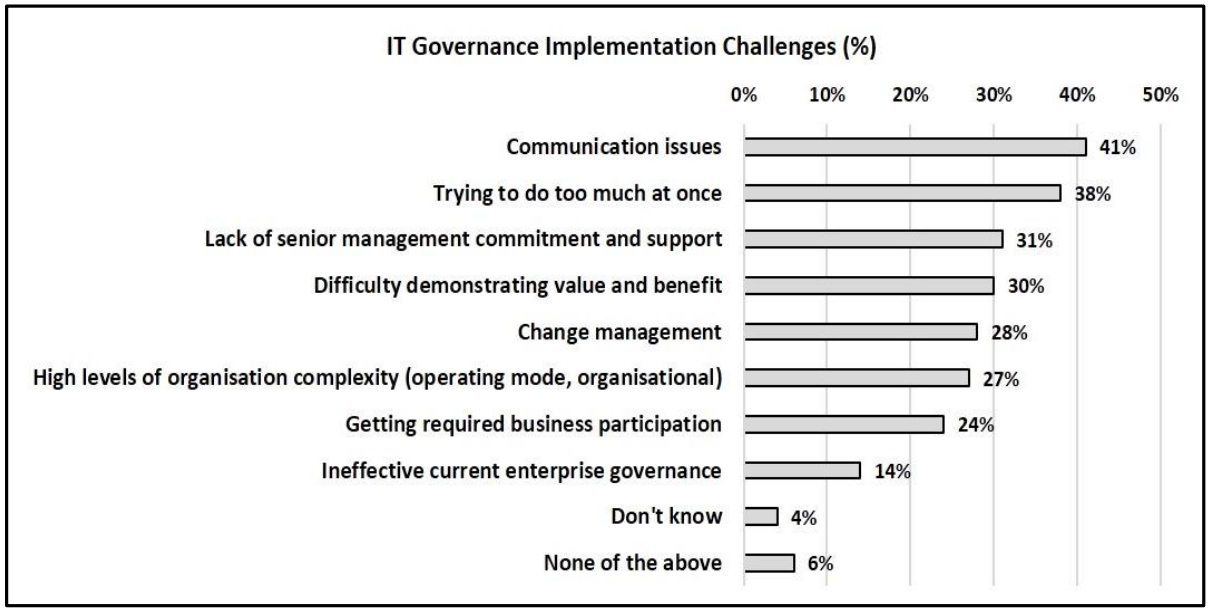


Figure 4-7 IT Governance Implementation Challenges (IT Governance Institute, 2011)

The implementation of any IT-enabled change, including the implementation of an IT governance or an IT control framework, usually requires significant cultural and behavioural change within the organisation *(IT Governance Institute, 2012).* Integrating formally autonomous digital functions and business units may involve changes in technology, business processes and the organisation *(Bowen, Chung & Rohde, 2007).* While such changes bring new opportunities, they also carry increasing risk *(IT Governance Institute, 2012).* To implement, mature, govern and realise value from an IT change initiative is a difficult, expensive, long, risky and hard journey, with no short cuts *(Ross, 2004).* It requires previously independent business and digital functions to spend significant time and money to conform to the new way of working *(Fonstad & Robertson, 2004).* IT governance is incorrectly believed to be a once-off event, such as compliance with a certain standard or framework, instead of a journey of change and improvement *(Raval & Dyche, 2012).*

4.4.3. Change benefits versus risk

Managers and staff of an organisation are usually ***not willing to accept the risks*** associated with a change in the ***absence of a compelling reason or business case*** to change *(Goss, Pascale & Athos, 1998)*. This business case may include a clear and inevitable risk to the organisation *(Goss, Pascale & Athos, 1998).* These risks include: 1) the risk to the current business operations; 2) the risk of personal failure; 3) the risk of having to make difficult decisions that will not satisfy everyone; and 4) the risk related to an uncertain and uncomfortable personal future *(Martin, 1998; East, 2011).* Members of an organisation are usually rewarded for reducing the risk to the current business operations *(Augustine, 1998)*. Even though the current operations should not be forgotten during a change initiative, it can be an obstacle for the change initiative when people have to choose between the new vision and self-interest *(Kotter & Schlesinger, 2008).* Cases for change sometimes serve as an end in itself, rather than addressing real pain points and weaknesses (*Kotter, 1995)*. Such cases for change do not address the practical, everyday issues being experienced *(Kotter, 1995).* Examples of such pain points for a digital environment include: 1) significant digital risks, security related incidents and regular audit findings; 2) failed digital changes or projects; 3) failure to meet regulatory requirements; and 4) service delivery problems *(IT Governance Institute, 2012).* The result is that 50% of change initiatives fail to establish an adequate sense of urgency to change *(Kotter, 1998).*

4.4.4. Lack of vision and roadmap

The inadequate sense of urgency to change is partially due to the lack of a clear, agreed and inspiring ***vision of the future or destination, a clear roadmap for the journey*** to reach the destination and some milestones along the way *(Augustine, 1998; Collins & Porras, 1998).* The lack of vision will result in a portfolio of uncoordinated projects that: 1) lead the organisation in different directions; and 2) will not collectively achieve the overall vision, or expected result, of the overall change initiative *(Kotter, 1998).* The leadership of the organisation will not embark on the change journey if they do not clearly see the vision and related value *(Ross, 2004).* Some organisations focus on activity-centric improvement programs consisting of an array of simultaneous isolated projects or actions, but without any short-term objectives or a clear link between the actions and the desired outcome *(Schaffer & Thomson. 1998)*. Such programs provide the promise of a long term improvement based on the

incorrect assumption that if the correct activities are performed today, then the required result will eventually be achieved *(Schaffer & Thomson. 1998)*. The result of such an approach is that: 1) support for the overall initiative and the momentum of the initiative are lost, because the benefit of the change is not evident to those involved in the improvement actions; and 2) short to medium term improvement opportunities are missed, because the organisation is focusing only on perfecting the long-term preparatory related work *(Kotter, 1995; Augustine, 1998).* Victory is also sometimes declared too soon and the pressure is removed before the change is embedded in the organisation's culture (i.e. "the way we do things around here") *(Kotter, 1995).* The result is that: 1) the situation regresses back to the previous state; or 2) the success is not followed up with a similarly challenging new vision and the momentum gained during the original change initiative is lost *(Collins & Porras, 1998; Kotter, 1998).*

4.4.5. Hard and soft factors

Seventy percent of change initiatives fail primarily because the organisations did not take a ***holistic approach, focusing on both the hard and soft factors*** required to see the change through *(Kotter, 1998).* The problems related to the ***"hard factors"***, or the project and program management dimension of change management, include the lack of: 1) the required capabilities; 2) formal commitment from top management; 3) financial and human resources; 4) an effective methodology or roadmap; 5) program oversight; and 6) frequent formal initiative reviews *(Sirkin, Keenan & Jackson, 2005; Manganelli & Klein, 1994).* The lack of a sufficiently powerful change coalition will cause: 1) a lack of critical mass in the organisation supporting and driving the change initiative; and 2) an increase in the momentum of those forces in the organisation who oppose the change *(Duck, 1998; Goss, Pascale & Athos, 1998).* There are also organisational barriers that are in conflict with the change, such as policies, structure and processes *(Kotter, 1998).* However, one of the primary root causes for change management related problems is the incorrect belief that mechanical measures (e.g. the "perfect" organisational structure; project management; improved policies and processes) will on their own ensure successful change *(Goss, Pascale & Athos, 1998).* This does not take into account that humans and their collective actions ultimately ensure success *(Augustine, 1998).* Such organisations completely ignore the human emotional aspect, or **"soft factors"**, which is at the heart of the change *(Duck, 1998).* For example, one of the significant root causes of change management failure is that those initiating the change and those affected by the change, perceive and assess the change differently (*Kotter & Schlesinger, 2008*). Those initiating the change see opportunities, either for the organisation or for themselves, whilst those impacted

by the change consider the change to be intrusive and disruptive *(Strebel, 1998).* Everyone needs to feel safe from harm and risk, including feeling safe from the change *(Duck, 1998).* Unfortunately this can seldom be offered by the organisation during a change initiative, due to: 1) a lack of predictability; and 2) a lack of understanding of the objectives and needs of the other parties involved in the change *(Duck, 1998).* If the emotional side is neglected, it leads to staff becoming suspicious, feeling de-valued, insecure and threatened *(Strebel, 1998).* This in turn results in staff becoming disengaged or leaving the organisation *(Strebel, 1998).* It can also lead to staff undermining the credibility of management and the change efforts, in order to preserve the past *(Augustine, 1998).*

4.4.6. Lack of trust

The ***lack of trust*** automatically emerges as a serious barrier and problem during any change initiative *(Duck, 1998).* It is partially due to isolated task teams and projects that create a communication vacuum *(Duck, 1998).* Conversations across organisational boundaries of isolated functions and across different levels of the organisational hierarchy, seldom happens *(Goss, Pascale & Athos, 1998).* This is caused by: 1) the application of a purely mechanical approach that breaks up the change effort into separate isolated pieces, without seeing the overall picture and the interrelationships between the pieces; 2) the limitation of narrow job descriptions and the unwillingness by staff, or discouragement by management, to work outside those boundaries; 3) the lack of knowledge about how an organisation really works; 4) an unspoken code of silence regarding the true organisational weaknesses; and 5) supressing confrontation or disagreement, because it is seen as challenging those in charge of the organisation *(Duck, 1998; Strebel, 1998; Goss, Pascale & Athos, 1998).* This leads to a lack of acknowledgement and revelation of the true organisational pain points and weaknesses that should be addressed during the change *(Goss, Pascale & Athos, 1998).* It is especially prevalent within large fragmented hierarchical organisations and bureaucratic public sector organisations (*van der Voet, 2014).* The lack of transparency and formal two-way communication regarding the vision and the change initiative causes misunderstanding, rumours, scepticism and cynicism *(Kotter & Schlesinger, 2008).* It finally leads to distrust between the members of the change team, as well as between those implementing the change and those impacted by the change *(Goss, Pascale & Athos, 1998; Duck, 1998).*

Individual managers of the organisation sometimes create additional problems by making demands and decisions that are contrary to, or undermine, the new agreed vision and related

change efforts ***("not walking the talk")*** *(Kotter, 1998).* The management of the organisation, or change leadership, loses credibility through such behaviour and this results in a lack of trust *(Strebel, 1998).* The result is that members of the organisation that have been through previous change initiatives become cynical towards the change initiative *(Duck, 1998).* Such people will go through, or survive, the change initiative without changing their behaviour *(Duck, 1998).*

4.4.7. Turf and territory

Organisational factors that could pose a significant problem for the collaboration efforts required by a change initiative, include: 1) the sometimes deep seated ***territorial behaviour*** in organisations; 2) the habit of ***protecting the "turf"*** of organisational units; and 3) an attitude of some organisational units that ***everything "done here" is always perfect***, whilst everything done by other organisational units are always flawed *(Goss, Pascale & Athos, 1998; Martin, 1998; Augustine, 1998).* In addition, IT departments are viewed in some organisations as merely a service provider, which reduces the importance of interaction, collaboration and communication between the IT function and the rest of the organisation *(Nfuka & Rusu, 2010).* This problem is further influenced by the project failure track record of IT. Approximately 31% of IT projects are cancelled before they are completed and only 9% of IT projects in large organisations are on average completed on time and within budget *(The Standish Group, 2014).* The high rate of IT project failure and lack of IT service delivery: 1) create a negative perception of the IT function within the organisation; 2) reduce trust in the IT function's capabilities; and 3) negatively impact on the credibility and reputation of the IT function *(Nfuka & Rusu, 2010).* Other digital functions may not be willing to collaborate with the IT function, or to make the IT function responsible for any of their critical digital solutions or services *(Nfuka & Rusu, 2010).*

4.5. Observations

Observations that relate to the generalised problems and influence the requirements of the artefact were made by the researcher, based on the base case and the literature review. These observations are presented in this section.

The size and complexity of the digital landscape of infrastructure asset intensive organisations is increasing as the convergence in digital technology is exploited and control system technology becomes more sophisticated. The problems related to the isolation of control systems and incompatible digital technology are reducing, due to the convergence in

technology and the development of digital standards. However, the incompatibility of new digital systems remains a risk that should be mitigated. The volume and variety of asset data required for strategic asset management decision making is continuously increasing. Fusing the asset data with value from across the digital landscape, to provide quality information in support of evidence-based decision making, is becoming a significant problem. The information security risk is increasing, including significant potential negative implications for control systems and the related critical infrastructure installations. This is due to the "weakest link" of the digital landscape being exploited, an increase in security threats, and an increase in the severity of the consequences of security failures. The low and inconsistent level of digital governance maturity within infrastructure asset intensive organisations is a problem. There is a lack of knowledge regarding the appropriate application of IT governance to digitised control systems. The over or under regulation of the digital environment is a problem. This is primarily due to a pure compliance approach to assurance, aiming at the highest level of maturity and complexity by default, or the notion that "one size fits all" when it comes to digital governance frameworks. It can potentially result in a high cost solution that does not deliver the expected value, because it does not mitigate the relevant risks. The segregation of IT and control system functions is common in large infrastructure asset intensive organisations. This can lead to a lack of clarity regarding roles, responsibilities and authority of digital functions in relation to an integrated digital landscape. It can further lead to a lack of communication, collaboration and knowledge sharing about important digital developments and risks. The typical change management related problems are relevant to the transition journey to implement digital governance. The primary problems include: 1) resistance to change; 2) a lack of a legitimate vision and an appropriate roadmap to achieve the vision; 3) ignoring either the "hard" or "soft" factors of the change; and 4) a lack of trust in the ability or intention of the digital function proposing and leading the change. When comparing the problems identified during the literature research and the problems abstracted from the base case, the overall observation is that the ***Rand Water problems are not unique*.** They are adequately reflected and represented in literature.

4.6. Requirements

The resolution of the generalised problems of the digital environment of a large and complex infrastructure asset intensive organisation, as described in this chapter, forms the basis of the requirements of the artefact.

The requirements of the artefact were identified by the researcher and are summarised per problem dimension as follows:

Requirement	Description
Technology and Information	
Reduce the risk due to the size and complexity of the digital landscape	Reduce the risk and increase the knowledge of the ever-increasing and sophisticated converged digital technology landscape of a large and complex asset intensive organisation, including facilitating the management of change to the digital landscape.
Ensure digital technology interoperability and integration	Ensure interoperability within the enterprise-wide digital landscape and enable asset data to be interfaced from control systems to IT systems for further processing and decision making.
Address dig data related problems of asset data	Reduce the risk related to big asset data (i.e. volume, variety and value), in order to provide quality asset information (i.e. completeness and correctness) in a timely manner and in the required format for evidence-based strategic asset management decision making.
Process	
Avoid under and over regulation	Avoid the negative implications of the under or over regulation of the digital environment, as well as the related digital governance notions of "compliance as an end in itself" and "one size fits all", via a balanced digital governance approach.
Provide a holistic approach to digital governance	Provide a holistic approach to digital governance, including the governance mechanism and operational process controls, or internal management controls, for the digital environment.
Consistent and appropriate digital governance	Ensure the consistent and appropriate application of digital governance and operational process controls to the enterprise-wide digital landscape and within all the IT and control system functions of the organisation.
Enable the exploitation of digital technology convergence with an acceptable level of risk	Enable the exploitation of the convergence in digital technology between IT and control systems (e.g. cost savings), but without increasing the risk to the infrastructure installations and the entire digital landscape beyond an unacceptable level.
Reduce information security risks	Reduce the ever-increasing information security related risks (i.e. availability, integrity, confidentiality) of the enterprise-wide digital landscape of the organisation. This includes the "weakest link" of a large and complex digital landscape (e.g. large distributed SCADA system using the internet).
People	
Improve sharing of common digital skills	Improve the sharing and utilisation of scarce common digital skills within a segregated organisation, required for an integrated and converged digital landscape.

Requirement	Description
Clarify roles, responsibilities and authority	Provide clarity regarding roles, responsibility and authority of the digital functions within a segregated organisation, in terms of digital systems, asset information, digital management processes and decision making.
Improve communication, collaboration and involvement	Improve communication, sharing of information or knowledge, and collaboration between all the digital functions of a segregated organisation, as well as involvement by all digital functions in enterprise digital initiatives.
Provide an agreed and clear vision and case for change	Provide a clear, shared, legitimate and formalised vision that all digital functions agree to. It should clearly define the target state and a compelling case for change (e.g. risks related to the current state; expected benefits).
Provide a roadmap to reach the future state	Provide a structured process, or road map, for all digital functions within the organisation to achieve the agreed vision, including quick wins and milestones along the way to maintain the momentum of the change initiative and to exploit short term opportunities.
Reduce resistance to change by improving trust	Address the resistance to change by improving the trust in the capabilities and intention of the digital function proposing and leading the change. This includes addressing the territorial and "turf protection" behaviour of digital functions
Reduce resistance to change by reducing the future state level of uncertainty	Reduce the resistance to change by reducing the level of uncertainty for all participating digital functions regarding the desired future state. In support of this, the artefact should ensure that the digital function proposing and leading the change "walk the talk" in terms of the new way of thinking and working.
Reduce resistance to change by improving communication and participation	Reduce the resistance to change by improving the participation of, and the two-way communication between, all the digital functions and the different levels of the organisation.
Provide an adaptable and flexible solution	Provide an adaptable and flexible solution that can be tailored to cater for changes to the organisation and to ensure that it is appropriate given the circumstances and context of the organisation.
Provide a sustainable solution	Provide a sustainable, reasonable and workable solution that will be accepted, embedded and operationalised by all the digital functions of the organisation.

Table 4-3 Requirements of the Artefact

Chapter 5 - Design of the Rand Water Way

The purpose of this chapter is to describe the artefact, namely a generalised integrated digital governance approach called "The Rand Water Way". The description of the Rand Water Way includes the overall philosophy, the underlying principles and the constituent parts of the approach. A more detailed description of the characteristics of the Rand Water Way is presented in Annexure A.

5.1. Philosophy and Principles

Transformation of a business comes about by changing the way the business thinks and works *(Pilling, 2010).* The Rand Water Way will be described in terms of four dimensions namely: the way of thinking, the way of working, the way of modelling and the way of controlling *(Seligmann, Wijers & Sol, 1989; de Vreede & Briggs, 2005).* The emphasis will be placed on the way of thinking and the way of working. The way of thinking illustrates the underlying principles or philosophy (i.e. value systems, basic premises) of the approach *(Seligmann, Wijers & Sol, 1989; de Vreede & Briggs, 2005).*

The overall ***philosophy*** of the Rand Water Way is that effective infrastructure asset management within a large, heterogeneous and complex organisation and digital environment requires asset information to be managed and utilised as an enterprise-wide resource. This in turn requires an enterprise-wide digital architecture and an optimal degree of enterprise-wide digital governance. These are introduced into the organisation in a manner that ensures a sustainable change to the way of working and the way of thinking about information management and digital governance.

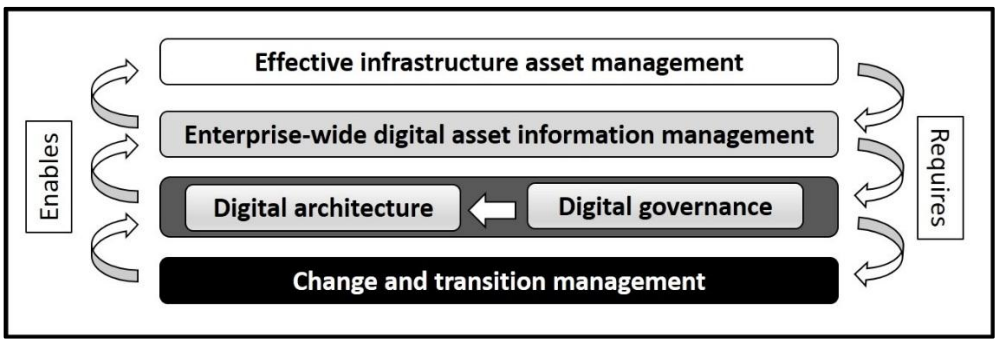


Figure 5-1 Overall Philosophy of the Rand Water Way

The underlying ***principles*** supporting the overall philosophy are as follows:

Principle	Description
Enterprise asset information resource	Asset information from across the digital landscape is recognised, managed and protected as a valuable enterprise resource, independent of its origin or format. It is harmonised and utilised to support effective evidence-based asset management related decision making.
Enterprise-wide digital landscape	The IT and control system landscapes are considered and managed as an integrated and secure enterprise-wide digital landscape. It enables asset information to flow in a secure manner between control and IT systems. It enables asset information from across the digital landscape to be exploited, whilst keeping the risk to the overall digital landscape or the core business operations, at an acceptable level.
Digital agility and enterprise-wide standardisation	An agile and standardised enterprise-wide digital architecture and related standards exist that are appropriate for a large, complex and heterogeneous digital landscape, that: 1) ensures interoperability within the digital landscape; 2) caters for future growth and expansion; and 3) caters for changes to business processes, requirements and the supporting digital technology solutions.
Risk-based "just enough" governance	Just enough risk-based digital governance and operational, or management level, process controls exist that avoid the under or over regulation of the environment, whilst adequately mitigating the inherent risk to: 1) the enterprise-wide digital landscape; and 2) the successful utilisation of asset information from across the digital landscape to enable effective asset management.
Sustainable cooperation and execution	Embedding the new way of working and the new way of thinking about the enterprise-wide digital landscape and digital governance within the organisation, in a manner that ensures: 1) the buy-in and cooperation of all digital functions of the organisation; and 2) the sustainable execution of digital governance and enterprise-wide asset information management.

Table 5-1 Underlying Rand Water Way Principles

The Rand Water Way and its constituent parts are represented as follows:

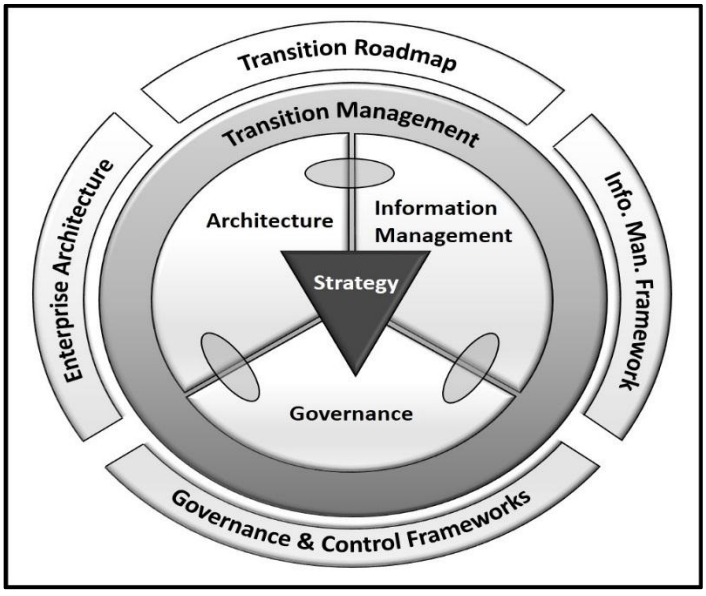


Figure 5-2 Rand Water Way Constituent Parts

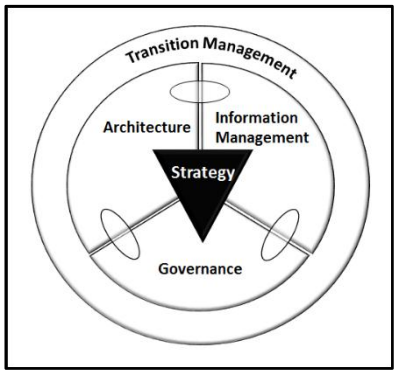
The representation depicts the key constituent parts of the Rand Water Way required to address and support the overall philosophy and underlying principles of the approach. The constituent parts of the framework are:

Component	Description
Strategy	The digital strategy(ies) that directs and formalises the Rand Water Way.
Information management	The enterprise-wide management of the digital asset information in support of effective asset management decision making.
Architecture	The enterprise-wide digital architecture and standards of the digital asset information and technology landscape.
Governance	The integrated and enterprise-wide digital governance and operational process controls for the digital asset information and technology landscape, required to enable effective asset information governance and architecture assurance.
Transition Management	The transition and change management approach for implementing the approach and introducing the new way of thinking and working to the organisation in a sustainable manner.

Table 5-2 Rand Water Way Constituent Parts

The constituent parts of the Rand Water Way do not exist in isolation. They overlap and are integrated. Examples of the overlap between the constituent parts are the disciplines of information governance, architecture governance and information architecture. The strategy and transition management constituent parts focus primarily on two of the dimensions of successful change, namely: 1) the people who will implement the change or who will be impacted by the change; and 2) the process of how the change will be achieved *(Anderson & Anderson, 2001).* The remainder of the constituent parts focus primarily on the third dimension, namely the content of the change (i.e. what needs to be changed) *(Anderson & Anderson, 2001).* Each of the constituent parts produces a related deliverable. The primary deliverables are a digital governance strategy, an information management framework, governance and control frameworks, an enterprise architecture, and a transition roadmap. Each of constituent parts are described, in order to illustrate the new way of working, controlling and modelling of the Rand Water Way. The emphasis of this research will be on the governance and the transition management constituent parts of the Rand Water Way.

5.2. Strategy



The purpose of this section is to describe the strategy constituent part of the Rand Water Way. It includes the description of the purpose of the strategy constituent part, alignment within an infrastructure asset management context, and the strategic themes related to the Rand Water Way.

The strategy constituent part is at the centre of the Rand Water Way. The ***purpose of the strategy*** constituent part is to provide direction to each of the other constituent parts of the Rand Water Way. It includes a description of the overall philosophy and underlying principles (the way of thinking) of the Rand Water Way. The objective of this constituent part is to: 1) provide direction to all relevant internal stakeholders, such as all the digital functions of the organisation; and 2) to communicate and obtain formal buy-in and commitment from executive management and the board for the digital technology related intention, aspirations, future direction and plans of the organisation, including the way of thinking (*Steensen, 2014).*

Strategic alignment is one of the IT governance focus areas *(ISACA, 2011; Leill-Cock, Graham & Hill, 2009).* The digital strategy is aligned to the corporate strategy, to ensure value delivery from digital technology investments and improved corporate performance through digital technology *(Charoensuk, Wongsurawat & Kang, 2014; Aversano, Grasso & Tortorella, 2012; Byrd, Lewis & Bryan, 2006).* An infrastructure asset intensive organisation should have an asset management strategy, or strategic asset management plan *(ISO, 2014).* The asset management strategy is aligned to the organisation's strategic goals and objectives (*ISO, 2014; Institute of Asset Management, 2008).*

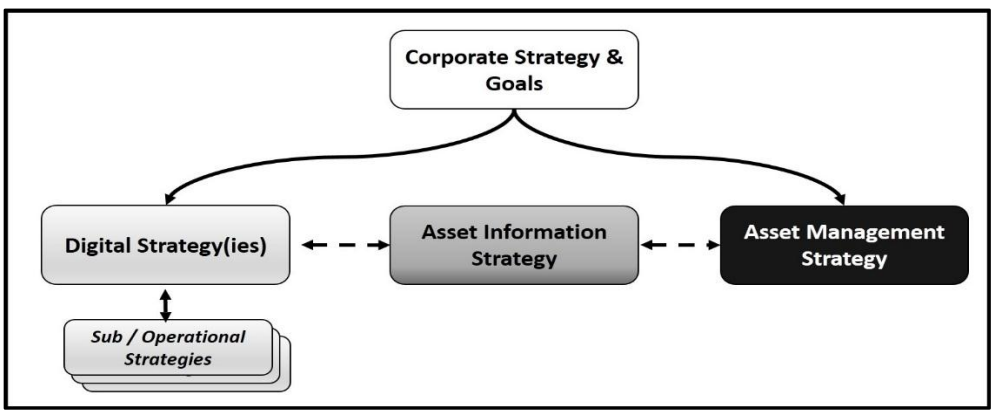


Figure 5-3 Strategy Alignment

In the context of an infrastructure asset intensive organisation, the digital strategy and the asset management strategy, are also aligned. This is to ensure that the digital functions and initiatives effectively support and enable the infrastructure asset management goals and objectives. The bridge, or link, that enables this alignment is the asset information strategy. It specifies the approach to the management of the asset information necessary to implement the asset management strategy *(Global Forum on Maintenance and Asset Management, 2011; Edwards, 2010).*

Some large and complex organisations consist of numerous business units and specialised departments, each with its own strategy *(Kaplan & Norton, 2001).* This includes segregated IT functions and control system functions, in the case of large and complex infrastructure asset intensive organisation *(The Water Environment Federation, 2007).* The digital strategies of these individual segregated digital functions should be linked, integrated or consolidated. This is required to create synergies and to overcome the traditional barriers to enterprise-wide strategy implementation, such as isolated functional silos and confusion regarding authority and responsibility *(Kaplan & Norton, 2001; Bowen, Chung & Rohde, 2007).* The same applies to enterprise-wide "super" digital strategies and sub / operational digital strategies within the organisation (e.g. a corporate digital strategy and a digital security sub/operational strategy) *(Kang, Lee & Kim, 2010).* These synergies are created via ***strategic themes*** and priorities that enable a consistent message and a consistent set of priorities to be used across, and at all levels of, the diverse, and sometimes dispersed, organisation *(Kaplan & Norton, 2001).* For this research, the common strategic themes relate to the philosophy and underlying principles (way of thinking) of the Rand Water Way. The strategic themes are as follows:

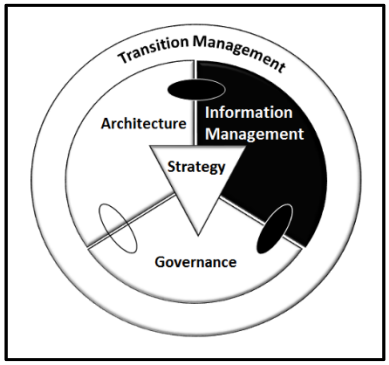
Theme	Description of related topics or questions
Operating model and convergence in digital technology (IT and control systems)	• The operating model to be applied for IT / digital functions, especially if there are numerous business units within the organisation. • How to address the convergence in digital technology, especially in terms of IT and control systems. Typical examples of options include centralised, federated or decentralised operating models or a hybrid (e.g. centralised governance and federated execution).
Management and governance of information	• How asset information resources should be managed, protected and governed to ensure that asset management decisions are effectively supported. • The scope of the information to be managed (e.g. life cycle stages, paper vs. electronic, structured vs. unstructured, internal vs. external sources).

Theme	Description of related topics or questions
Enterprise architecture objective, role and overall direction	• What the objectives, role and content of the enterprise architecture and related standards should be and how it should be governed to ensure the necessary agility of the digital landscape, address the complexity of the environment, and address change in the environment. • Should the IT landscape be a wall-to-wall single product solution (e.g. ERP), a collection of best-in-class solution, or something in between (hybrid, best-fit)?

Table 5-3 Enterprise Digital Strategy Themes

These strategy themes represent three of the constituent parts of the Rand Water Way, namely: information management, governance, and architecture. In addition, the current situation, a desired future state (vision), and a high level strategic plan to achieve the future state should be defined in the digital strategy for each of the strategic themes *(Kluth, Jäger, Schatz, & Bauernhansl, 2014; Kotter, 1998; Geum, Lee & Park, 2014).* A maturity model can be used to assess the current practice, determine and communicate the appropriate future state and identify the improvements required to achieve the future state *(Wendler, 2012; Humphrey, 1989; Pilling, 2010; Leitão, Cunha, Valente & Marques, 2013).*

5.3. Information Management



The purpose of this section is to describe the information management constituent part of the Rand Water Way. It describes the purpose and benefit of information management in support of infrastructure asset management, the scope and content of an enterprise information management framework, as well as the information management activities.

Information management is one of the key enablers of infrastructure asset management and is therefore one of the constituent parts of the Rand Water Way *(ISO 2014; Institute of Asset Management, 2008).* The ***purpose*** of information management in support of effective infrastructure asset management is to enable strategic long-term asset decisions, utilising evidence-based multi-stakeholder group decision making *(Zhang & Guo, 2014; Matrosov, Woods & Harou, 2013; Keen & Sol, 2008).* This is achieved by ensuring that: 1) relevant, meaningful, quality, timely asset information is delivered to the right people in the right format and at the right time to make asset decisions; and 2) that the asset information has been unified, harmonised or fused, from information sources across a large, complex and heterogeneous

digital landscape *(ISO, 2014; Fernández-de-Alba, Fuentes-Fernández & Pavón, 2013; Lehman & Heagy, 2014; Lloyd, 2012).* Asset information is a strategic corporate resource and should be managed, governed, controlled, protected and utilised accordingly, in order to ensure the integrity and availability of the required information in a timely manner *(Silva, de Gusmão, Poleto, e Silva, & Costa, 2014; Uçaktüçrk & Villard, 2013).* It is therefore important to address any underlying asset information related problems, including data quality and big data related problems *(Burns, 2010; von Petersdorff, 2013).* This includes: 1) increasing data volumes; 2) increasing data format and media variety; and 3) selecting asset information with decision making value at an acceptable information management cost *(Chang, Kauffman & Kwon 2014; Edwards, 2010).* Information management defines to some degree the way of modelling of the Rand Water Way in terms of information architecture and information modelling languages, standards and notations. It also defines to some degree the way of working in terms of the asset information management and governance related activities.

An ***enterprise information management framework*** (EIMF) in support of infrastructure asset management is an enterprise-wide framework. It is co-created and applies to all the digital functions of the organisation and all the IT and control systems. The EIMF addresses all he information management elements required to define how asset information will be managed in order to enable information exchange and exploitation, in support of effective asset management decision making. These are: 1) the asset information life cycle; 2) asset data format scope; 3) the asset information management activities; and 4) the trusted internal and external asset information sources.

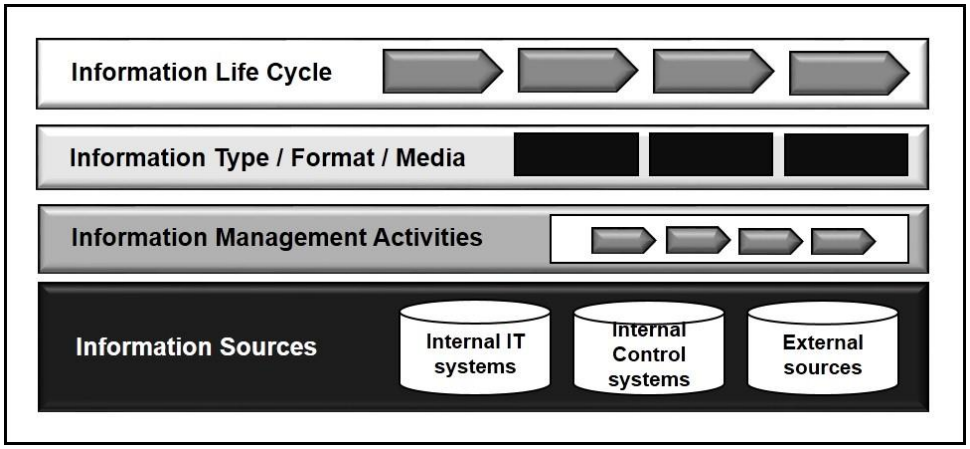


Figure 5-4 Enterprise Information Management Framework

All digital asset information with decision making value, independent of its format or origin, is managed and controlled throughout the defined information life cycle, from creation to

disposal, *(Iyamu, 2011; Institute of Asset Management, 2008; Association of Information and Imaging Management, 2014).* The EIMF covers all digital asset information of the organisation, including structured and unstructured asset information created via the organisation's digital systems, or originating from trusted external sources *(Chang, Kauffman & Kwon, 2014; ISO 2014; Chen & Zhang, 2014).* A catalogue of authentic trusted asset information sources from internal and external to the organisation, is defined to verify the origins of authentic asset information to be utilised for decision making *(Iyamu, 2011; ISO, 2014).* The information management related activities are the minimum activities to be performed to effectively manage asset information throughout its life cycle, in order to deliver value in support of infrastructure asset management decisions *(IT Governance Institute, 2012; Kooper, Maes & Lindgreen, 2011).* These activities are divided into two groups, namely: 1) the core activities directly related to the management of asset information; and 2) the non-core services that are closely related to other disciplines.

The core asset information management activities are:

Activity	Description
Information architecture & standards management	Management of the asset information architecture, taxonomy (i.e. semantics, terminology, and data definition language), information related standards, and meta-data *(Kluth, Jäger, Schatz & Baurenhansl, 2014; Zandi & Tavana, 2012).*
Information ownership management	Identification and allocation of asset information ownership, stewardship or custodianship for all asset information across the digital landscape required for asset management decisions *(Iyamu, 2011; Ross, 2004).*
Information security and risk management	Management of asset information security and operational information risk, including business continuity, to protect the integrity, confidentiality and availability of the required asset information *(Webb, Ahmad, Maynard & Shanks, 2014; Rice. & Almajali, 2014).*
Information quality management	The management of the quality of all asset information, including master and transactional data. This includes data accuracy, completeness and consistency *(Kwon, Lee & Shin, 2014; Anwar & Mahmood, 2014).*

Table 5-4 Core Asset Information Management Activities

Some of the non-core information activities relating to other disciplines are:

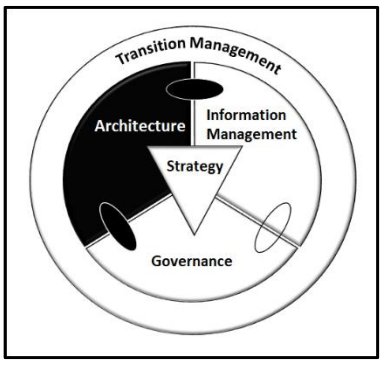
Activity	Description
Records & document management	Asset records and document management, including information preservation. It focuses primarily on unstructured asset information, such as content, documents and images *(ISO, 2001; Association of Information and Imaging Management, 2014).*

Activity	Description
Compliance management	The management of compliance to all relevant standards, frameworks, codes and legislation, such as the protection of personal information and privacy related legislation. (*Kooper, Maes & Lindgreen, 2011; ISO, 2001).*
Explicit knowledge management	Explicit knowledge management, as a subset of knowledge management, focusing on documented, recorded or captured asset related knowledge (*BSI, 2003; Madsen, 2013).*
Information classification & categorisation	Asset information classification and categorisation, relating to information security and compliance management. It addresses information sensitivity levels, as well as personal information *(Iyamu, 2011; Hammoudech & Newman, 2013).*

Table 5-5 Non-Core Asset Information Management Activities

There is an ***overlap and integration point*** between the information management and governance constituent parts of the Rand Water Way, namely information governance. It specifies the accountability for the management of an organisation's asset information *(Association of Information and Imaging Management, 2014).* Information governance establishes accountability, rules and decision-making rights for the valuation, creation, collection, analysis, distribution, storage, use and control of asset information *(Kooper, Maes & Lindgreen, 2011).* It is an umbrella function for legislative compliance and records management related to asset information *(Sheperd, Stevenson & Flinn, 2010).* There is also an overlap and integration point between the architecture and information constituent parts of the Rand Water Way, namely the information architecture and related standards. This will be described in the architecture section.

5.4. Architecture



The purpose of this section is to describe the architecture constituent part of the Rand Water Way. It describes the purpose and benefit of an enterprise architecture and related standards in support of enterprise information management, the enterprise architecture scope and content, architecture governance and the information architecture.

The ***purpose and benefit*** of an enterprise architecture in support of enterprise information management and infrastructure asset management includes: 1) reducing digital landscape related risk; 2) enabling asset information harmonisation and exploitation; 3) enabling digital landscape change and innovation; 4) improving digital function alignment; 5) increasing the

knowledge of the digital landscape; and 6) reducing cost. The enterprise architecture and related standards are key, in order to deal with the risk related to the complexity, size and heterogeneous nature of the digital technology environment of an infrastructure asset intensive organisation *(ISO, 2014; Kluth, Jäger, Schatz & Baurenhansl, 2014).* One of these risks is the lack of interoperability within the digital landscape, especially between IT and control systems *(The Open Group, 2009; The Water Environment Federation, 2007).* The enterprise architecture assists in improving the knowledge and understanding of the organisation and its digital landscape *(Šaša & Krisper, 2011; Kang, Lee, Choi & Kim, 2010).* It further assists in presenting and communicating the digital landscape to all stakeholders across the different functions and levels of the organisation, including the segregated digital functions *(Nolan & McFarlan, 2005).* An agile enterprise architecture is required to cater for the fast pace of digital technology change at an asset intensive organisation, including "smart" technologies and the convergence in digital technology *(Global Water Intelligence, 2013; Federal Energy Regulatory Commission, 2013).* It enables the organisation to innovate, transform or respond to opportunities and change in a controlled manner *(Rice & Almajali, 2014; Zachman, 2003).* The Enterprise Architecture assists the organisation to select and achieve a common digital future, as well as achieve digital strategy alignment between the digital solutions and functions *(Šaša & Krisper, 2011; Kang, Lee, Choi & Kim, 2010).* This is achieved by agreeing on the desired digital future state (vision architecture), analysing the impact of the change across the digital landscape, and agreeing on the transition plan to achieve the desired future state via a prioritised portfolio of projects *(Agievich & Skripkin, 2014; Giachetti, 2012).* The enterprise architecture will further assist with cost saving for the organisation, due to the standardisation and consolidation of the converged digital infrastructure and the related sharing of critical and scarce digital skills and resources *(Ross, 2004).*

The ***scope*** of the Enterprise Architecture in support of infrastructure asset management, includes both the IT and control system landscapes and all the responsible digital functions across a large infrastructure asset intensive organisation. The ***content*** of the enterprise architecture includes the business architecture, technical architecture and information architecture, as well as the current and future state architectures (*Šaša & Krisper, 2011; The Open Group, 2009).* The information architecture, also referred to as the information systems architecture, includes the asset data and asset related application architectures *(Iyamu, 2011; The Open Group, 2009).*

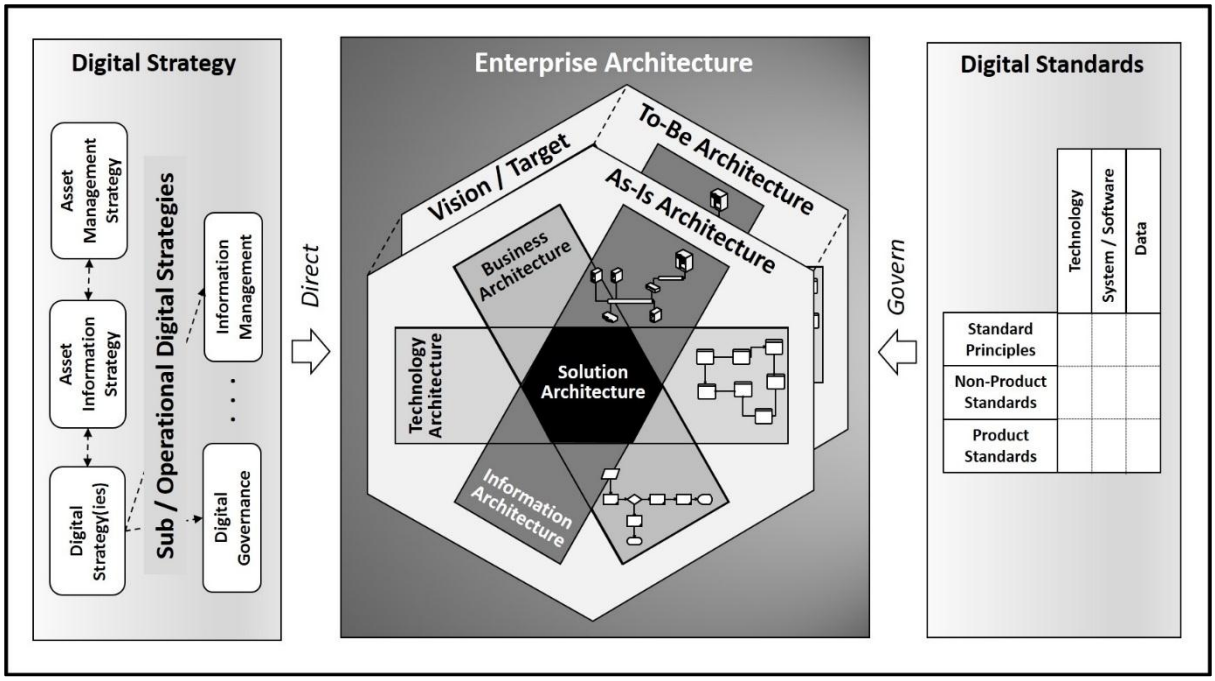


Figure 5-5 Digital Architecture and Standards

An enterprise information security architecture supplements the generic enterprise architecture views to address information, or cyber, security threats to the digital landscape *(Anwar & Mahmood, 2014; Wang & Shuo, 2013).* This includes the security threats to the "weakest link" of large distributed SCADA systems, implemented on a converged integrated digital infrastructure platform *(Rice & Almajali, 2014; Campbell, 2011).* The various enterprise architecture frameworks (e.g. TOGAF, Zachman), and meta-models, as well as the associated architecture modelling standards, conventions or languages (e.g. IEEE 1471-2000, UML, ISO 2008) represent the primary way of modelling of the Rand Water Way *(Zandi & Tavana, 2012; ISO, 2008).*

Architecture governance is the ***overlap, or integration point***, between the architecture and governance constituent parts of the Rand Water Way. The enterprise architecture is governed at an enterprise-wide level *(Ross, 2004; The Open Group, 2009).* This is performed via defined minimum digital standards and the related selection and assurance processes, which all digital functions agree to and comply with *(IT Governance Institute, 2012; Zachman, 2003).* The standards include technology standards, software standards, and information standards *(The Open Group, 2009; Ross, 2004).* The standards are required to effectively address the possible lack of interoperability, incompatibility or the inability of digital solutions to communicate with other one another *(ISO, 2014; Šaša & Krisper, 2011).* The standards could also include industry standards, such as secure network protocols and data exchange standards

for control systems, in order to improve security and interoperability *(Soloman, 2010; Campbell, 2011).* Architecture governance is supported by a structured process for the evaluation, selection and inclusion of digital standards into the organisation's enterprise architecture *(The Water Environment Federation, 2007).*

The ***information architecture*** is the ***overlap and integration point*** between the architecture and information constituent parts of the Rand Water Way. The enterprise-wide information architecture identifies and defines the complete digital systems and database landscape that enables the organisation to collect, retain, analyse, transform, disseminate and exploit asset information, as well as the relationship between these systems and databases *(Kluth, Jäger, Schatz & Baurenhansl, 2014; Zandi & Tavana, 2012).* It enables asset information exchange between digital systems *(Soloman, 2010; von Petersdorff, 2013)*. This is achieved by ensuring that: 1) the wealth of asset data stored and processed by digital systems is accessible to users and other digital systems; 2) the knowledge of the asset data and the relationship amongst data elements is improved; and 3) asset data across the digital systems landscape is unified through consistent semantics or terminology and data definitions *(Iyamu, 2011; ISO 2014).* The inclusion of control systems is illustrated using a 4-layer information architecture:

	Layer	Description
1	**Information exploitation**	Asset information from across the digital systems landscape is utilised, or exploited, for decision making purposes.
2	**Information exchange**	Asset information is exchanged between digital systems within the information generation and exploitation layers.
3	**Information generation and processing**	Asset information is created or generated.
4	**Digital infrastructure**	Enables levels 1 to 3 to store, process, communicate and print data, or information.

Table 5-6 Systems Architecture Layers

The new components of this information architecture are the control systems and the related instrumentation. The control systems (e.g. SCADA) and their database (e.g. Data Historian) fit into the information generation and processing layer *(Soloman, 2010).* The majority of the information generated by a control system originates from the instrumentation linked to the control system, rather than people (e.g. "smart" devices, programmable logic controllers, sensors). *(Kiameh, 2003; Global Water Intelligence, 2013; ISO 2014).* These instruments are considered both part of the information generation layer and the supporting digital infrastructure layer.

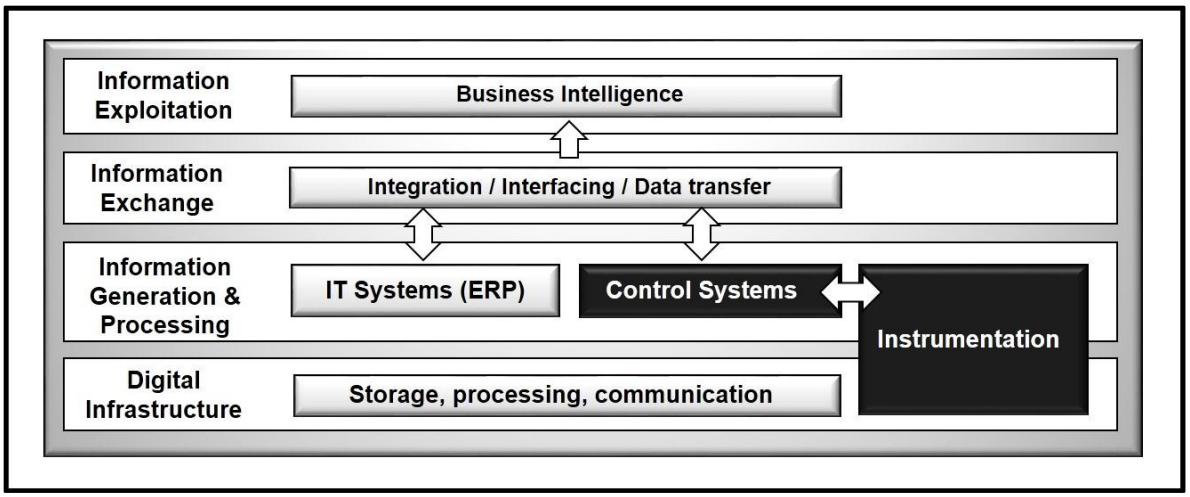
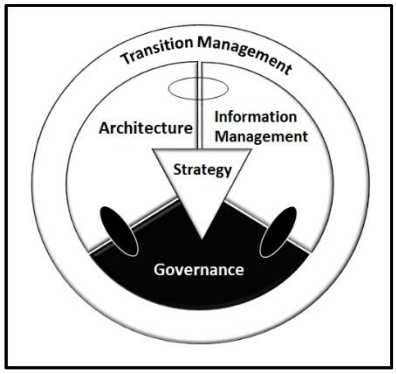


Figure 5-6 Four Layered Systems Architecture

It is the aim of the information architecture to collect asset data automatically and once-off, where possible and feasible, via control systems, rather than recapturing it in IT systems *(The Water Environment Federation, 2007).*

5.5. Governance



The purpose of this section is to describe the governance constituent part of the Rand Water Way. It includes the description of the purpose of the governance constituent part, the holistic approach to digital governance, the digital governance framework, as well as the selection and prioritisation of digital governance mechanisms and operational process controls.

The ***purpose*** of the governance constituent part of the Rand Water Way is to assist asset intensive organisations to: 1) achieve their infrastructure asset management related goals; 2) deliver value through effective governance and management of digital technology and asset management related information; 3) encourage desirable behaviour in the use of digital technology, and 4) create optimal value from digital technology by optimising the balance between value delivery and risk *(IT Governance Institute, 2012; Verhoef, 2007; ISO, 2008; ISACA, 2012).* Digital governance, within the context of the Rand Water Way, is defined as the system by which the current and future use of IT, control systems and digital asset information, is effectively and efficiently directed and controlled at an enterprise level to support the organisation, optimise value and risk, and enable the achievement of the organisation's infrastructure asset management objectives and plans *(Adapted from ISO, 2008;*

Institute of Directors of South Africa, 2009; and IT Governance Institute, 2012). The governance constituent part represents the way of controlling and the way of working of the Rand Water Way, in terms of the digital governance mechanisms and operational process controls to be implemented.

A ***holistic approach*** is adopted for digital technology and asset information governance in support of asset information management and enterprise architecture assurance *(IT Governance Institute, 2012).* Both the governance level (macro level) and operational management level (micro level) of the hierarchical governance framework are addressed *(von Solms & von Solms, 2006; Kooper, Maes & Lindgreen, 2011).* This includes the digital strategy, decision making authority, policies, performance management, governance structures, compliance, digital organisation, digital technology architecture, as well as governance and operational processes *(Benaroch, Chernobai & Goldstein, 2012; ISACA, 2012).* This approach takes all digital functions into account, as well as the related digital processes, services and risks *(Gheorghe, 2010; IT Governance Institute, 2012).* It ensures that the benefits of the strategic digital governance level flows down to the operational digital management level of the various digital functions *(Prasad, Heales & Green, 2010; Kluth, Jäger, Schatz & Baurenhansl, 2014).*

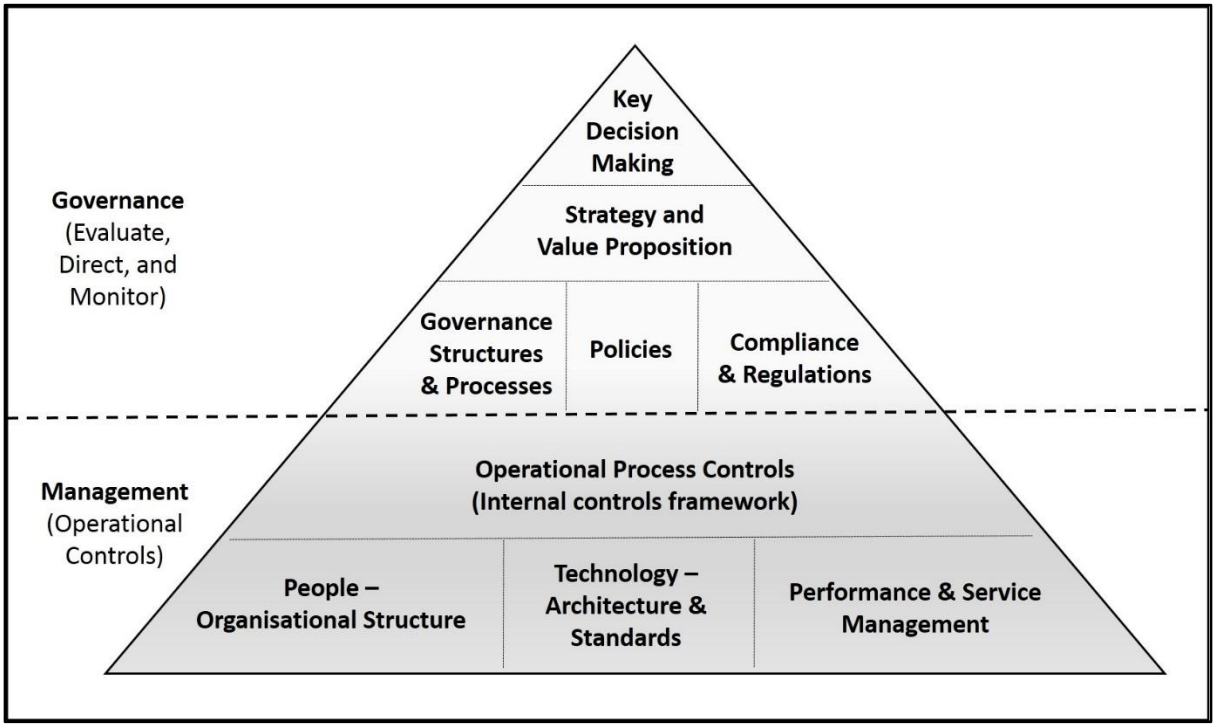


Figure 5-7 Holistic Approach to Digital Governance

The result is the enterprise-wide operationalisation of digital governance via aligned standardised operational process controls related to the planning, building, running and

monitoring of digital services and products *(Prasad, Green & Heales, 2012; Benaroch, Chernobai & Goldstein, 2012).*

A ***digital governance framework*** is defined, agreed and implemented, consisting of the required governance structures and processes *(Bowen, Chung & Rohde, 2007; Institute of Directors of South Africa, 2009).* A strong, effective and clear structure of digital governance, including decision making, is an important component of digital governance in a large, complex heterogeneous organisation *(Weill & Ross, 2004; van Grembergen, de Haes & Guldenstops, 2004).* The digital governance structures are supported by digital governance processes that comply with the established policies *(Bowen, Chung & Rohde, 2007; Kaplan, 2005).* The governance structures specify the board level committees (macro) and management level structures (micro) that have any accountability or responsibility regarding digital technology and information governance *(Kooper, Maes & Lindgreen, 2011; Ross, 2004).* This includes structures such as the audit and risk sub-committee(s) of the board, the executive management committee, the digital steering committee, the various digital functions, as well as digital projects and programmes *(Fonstad & Robertson, 2004; Institute of Directors of South Africa, 2009).*

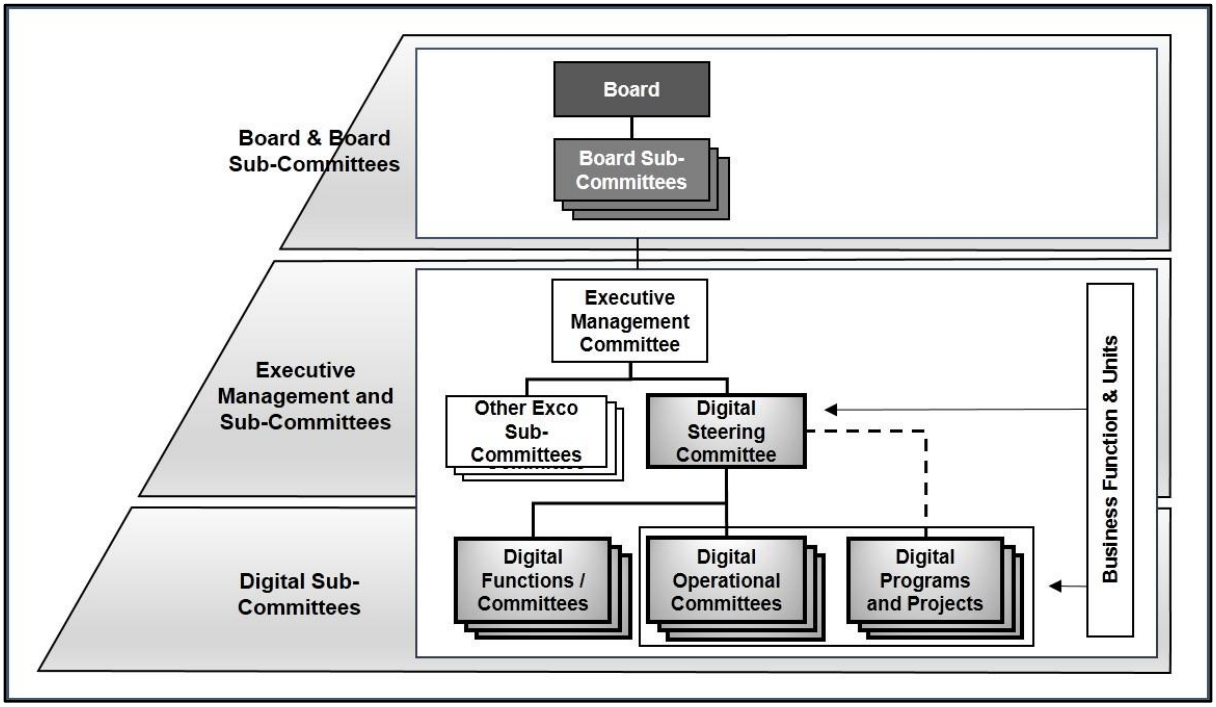


Figure 5-8 Digital Governance Structure

The digital steering committee is the most prominent governance structure of the organisation *(Prasad, Green & Heales, 2012).* It is tasked with business and digital strategy alignment, value delivery and risk management for all digital functions of the organisation *(Bowen, Chung &*

Rohde, 2007; Prasad, Heales & Green, 2010). Over and above the governance role, these structures can also play an important role as an engagement, information sharing, communication and change management platform for the various segregated digital functions of the organisation *(Nfuka & Rusu, 2010; Flores, Antonsen & Ekstedt, 2014).* The following are the key characteristics of a digital governance structure, to successfully support infrastructure asset management in a large, complex, heterogeneous organisation:

Requirement	Description
Enterprise-wide and centralised	Digital governance is centralised to ensure enterprise-wide coverage, including all digital functions, solutions and asset information of the organisation, including connections between corporate and business unit digital governance *(Weill & Ross, 2004; Sambamurthy & Zmud, 1999).*
Clarity of accountability and responsibility	The digital governance related accountability, roles and responsibility of the digital functions and governance structures, are clearly and unambiguously allocated and defined (e.g. RACI matrix, charter, terms of references) *(Prasad, Green & Heales, 2012).* Digital governance processes are defined to embed digital governance accountability and responsibility into the organisation *(Bowen, Chung & Rohde, 2007).* This is crucial in a large, complex, multi-business or digital unit organisation, especially when digital governance is considered as a shared responsibility *(Prasad, Green & Heales, 2012; Bowen, Chung & Rohde, 2007).*
Integrated governance	The digital governance structure is integrated into the corporate governance structure and share mechanisms or structures with other governance processes, where relevant *(Weill & Ross, 2004; IT Governance Institute, 2012).* This is done because: 1) digital technology and asset information governance is a subset discipline of corporate governance; and 2) digital technology and information are linked to other key enterprise assets (e.g. financial, human, intellectual property) *(Kooper, Maes & Lindgreen, 2011; Gheorghe, 2010).*
Appropriate mix and active participation	The digital governance structures at the management level are co-created *(Prasad, Green & Heales, 2012).* They include and formalise the appropriate mix of active participation from different levels of the organisation, as well as from segregated business and digital functions across the organisation (i.e. IT and control systems) *(Prasad, Heales & Green, 2010; Ross, 2004).* The digital steering committee should be chaired by a member of the organisation's leadership to ensure top management involvement and commitment *(Tohidi, 2011).* This will assist in: 1) promoting a shared understanding and knowledge; 2) utilising the relevant expertise from across the organisation; and 3) ensuring continued active participation and commitment from all relevant internal stakeholders *(Heales & Green, 2010; Prasad, Green & Heales, 2012).*

Requirement	Description
Operationalisation of digital governance	Digital function management committees (i.e. IT and control system functions) and operational committees focusing on key subjects or controls (e.g. change control committee, architecture review committee) are included in the digital governance structure definition *(Fonstad & Robertson, 2004).* This will ensure that decisions made by the higher level governance structures will flow down to the operational digital control level and the various digital functions *(Benaroch, Chernobai & Goldstein, 2012; Gheorghe, 2010).* The result is the operationalisation of enterprise-wide digital governance and alignment *(Kluth, Jäger, Schatz & Baurenhansl, 2014).*
Collaboration and information sharing platforms	The digital governance structure includes platforms for digital technology related collaboration, engagement, change management, consensus building and knowledge sharing between segregated digital functions and across the different levels of the organisation *(Hadaya & Cassive, 2012; Flores, Antonsen & Ekstedt, 2014).* This is key to the success of the efforts to integrate previously autonomous digital functions. It creates: 1) change advocates or champions: 2) a change coalition; and 3) a critical mass for the change initiative *(Kotter & Schlesinger, 2008; Othman, Chan & Foo, 2011).* It is a critical aspect of team work, with the purpose to align the goals of the individual digital functions to that of the team as a whole *(de Vreede & Briggs, 2005).* It will further improve the knowledge of the participants and reduce risk (e.g. knowledge of latest security threats) *(Campbell, 2011; Anwar & Mahmood, 2014).*

Table 5-7 Digital Governance Structure Characteristics

Digital governance and operational process controls are ***selected and prioritised*** to ensure that they are optimal, appropriate and useful to effectively enable enterprise-wide information management in support of effective infrastructure asset management in the context of a large, complex, heterogeneous asset intensive organisation *(Liell-Cock, Graham & Hill, 2009; Pilling, 2010).* The following are the key characteristics of the proposed selection and prioritisation approach:

Requirement	Description
"One size fits all" myth	The myth of a "one size fits all" solution, without the possibility of deviation or adaption, is avoided *(Verhoef, 2007; Institute of Directors of South Africa, 2009).* This is achieved by selecting and tailoring "best practice" frameworks and standards to be useful and cost effective, whilst still achieving the digital governance and management objectives *(Pilling, 2010; IT Governance Institute, 2012; Bowen, Chung & Rohde, 2007).*

Requirement	Description
Beyond compliance	The implementation and application of digital governance and operational controls go beyond once-off compliance to any external standard, framework, code or best practice *(Pilling, 2010).* It does not treat compliance as an end in itself *(Raval & Dyche, 2012).* This ensures that the selected controls reduce risk, are cost effective and add value to the organisation *(Port & Wilf, 2014).* It also ensures that assurance can be provided in terms of the adequacy of the controls *(Matwyshyn, 2009).*
Balanced regulation	A balance is achieved between cost, value and risk in terms of the degree of digital governance and operational control *(Campbell, 2011; Webb, Ahmad, Maynard & Shanks, 2014).* This includes information security related controls, such as disaster recovery and identity management *(ISO, 2005; Shamala, Ahmad & Yusoff, 2013*). Risks are adequately mitigated, whilst still delivering, or creating, value for the organisation *(IT Governance Institute, 2012; Kerr & Murthy, 2013).* The approach will avoid the negative impact on the organisation, due to under regulation (i.e. increased risk) and over regulation (i.e. efficiency, productivity, cost and time to market) *(Verhoef, 2007).*
Risk-based prioritisation	The prioritisation of controls is performed using a risk-based approach *(ISO, 2005; Shedden, Ruighaver & Ahmad, 2010).* The focus is placed on more critical governance mechanisms and operational controls *(Webb, Ahmad, Maynard & Shanks, 2014; Kerr & Murthy, 2013).* This will ensure that limited and scarce resources and expertise are utilised effectively, whilst the high value and most critical asset information and related digital technology are protected from high-risk scenarios *(Zhiwei & Zhongyuan, 2012; Shamala, Ahmad & Yusoff, 2013; Feng, Wang & Li, 2014).*

Table 5-8 Control Prioritisation Approach Characteristics

The appropriate, or "just enough", governance mechanisms and operational process controls are selected and prioritised, based on the principle that the higher the risk associated with the absence of the control: 1) the higher the degree of control centralisation, or regulation; and 2) the lower the degree of flexibility and autonomy of the digital functions of the organisation in relation to that control.

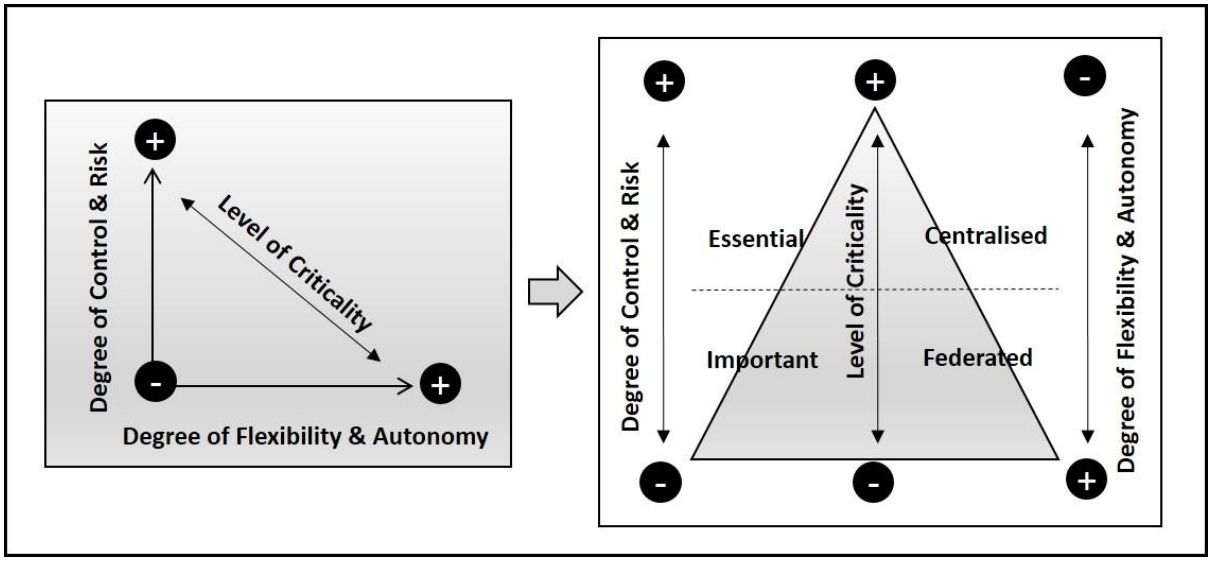


Figure 5-9 "Just-enough" Control Selection and Prioritisation Approach

Digital governance and internal operational process controls are prioritised based on their level of criticality and are categorised as either important or essential. Unimportant controls are not considered relevant for the purpose of this approach. The two categories of controls are implemented and executed as follows:

Control Criticality	Implementation and Execution Approach
Essential	The management and execution of essential controls are centralised across the digital environment and executed in exactly the same manner using a single process and single accountable governance structure.
Important	Important controls are governed by a common policy(ies), but can/may be executed on a federated basis by the respective digital functions.

Table 5-9 Implementation of Essential versus Important Controls

The two inherent risks used as a basis for determining the criticality of the controls are:

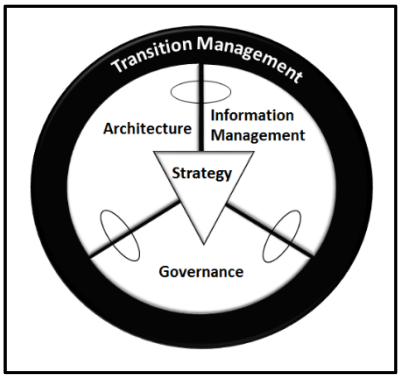
Risks	Description
Decision support risk	The risk that the required quantity and quality asset information from across the digital landscape cannot be made available to the right people at the right time, in a usable format and in a sustainable manner, in order to make the required infrastructure asset management decisions.
Digital landscape risk	The risk of failure or service interruption of the overall digital environment and/or the core business operations, due to the integrated and converged nature and the interconnectivity of the IT and control system landscapes.

Table 5-10 Risk Definition for Risk-based Control Prioritisation

The root causes of these two inherent risks are identified, and the contribution of the root causes to the risks are assessed. Those controls that address the primary and most significant root causes of these two risks will be considered as essential controls, and the remainder will be considered as important controls *(Tohidi, 2011).*

The governance constituent part of the Rand Water Way ***overlaps and integrates*** with the information management and architecture constituent parts. These integration points are information governance and architecture governance. Both these topics were described in the information management and architecture sections respectively.

5.6. Transition Management



The purpose of this section is to describe the transition management constituent part of the Rand Water Way. It describes the purpose of the transition management constituent part, the transition roadmap and the supporting work streams. The supporting work streams include the bedrock factors, project and program management and organisational change management.

The ability to execute the digital strategy is as important, if not more important, than the quality of the strategy itself *(Kaplan & Norton, 2001).* The ***purpose*** of the transition management constituent part of the Rand Water Way is: 1) to effectively foster, introduce and implement a new way of thinking and working in relation to asset information management and digital governance in support of infrastructure asset management; and 2) to do so in a sustainable way that does not cause disruption to, or have unnecessary negative implications for, the operational digital processes or the core business of the organisation *(Lloyd, 2012; ISACA, 2012; IT Governance Institute, 2011).* The transition management constituent part describes the transition journey in terms of the phases and activities to be performed in a holistic approach, including the mechanical and human perspectives required to see the change through *(Kotter, 1995 & 1998; East 2011).* It addresses two dimensions of successful transition management, namely: 1) the people who will implement the change or be impacted by the change; and 2) the process of how the change will be achieved *(Anderson & Anderson, 2001).* The transition management constituent part primarily describes the way of working of the Rand Water Way. It also describes the way of controlling the work to be performed during the journey.

The transition management constituent part ***consists*** of two levels, namely: 1) the transition roadmap; and 2) three supporting work streams.

The ***transition roadmap*** provides a structured and time-based approach for the long-term digital governance strategy implementation in support of infrastructure asset management *(McDowall, 2012; Geum, Lee & Park, 2014).* It defines how the transition can be successfully achieved in a large and complex infrastructure asset intensive organisation *(Anderson & Anderson, 2001; East, 2011; Soloman, 2010).* It does not offer any "short cuts", but includes some milestones (e.g. "quick wins") along the way to illustrate value and to maintain the change momentum, without increasing the risk to an unacceptable level *(Anderson & Anderson, 2001).* The transition roadmap represents the primary way of working of the Rand Water Way, by specifying the work to be performed (i.e. phases, stages, activities) to achieve the agreed vision.

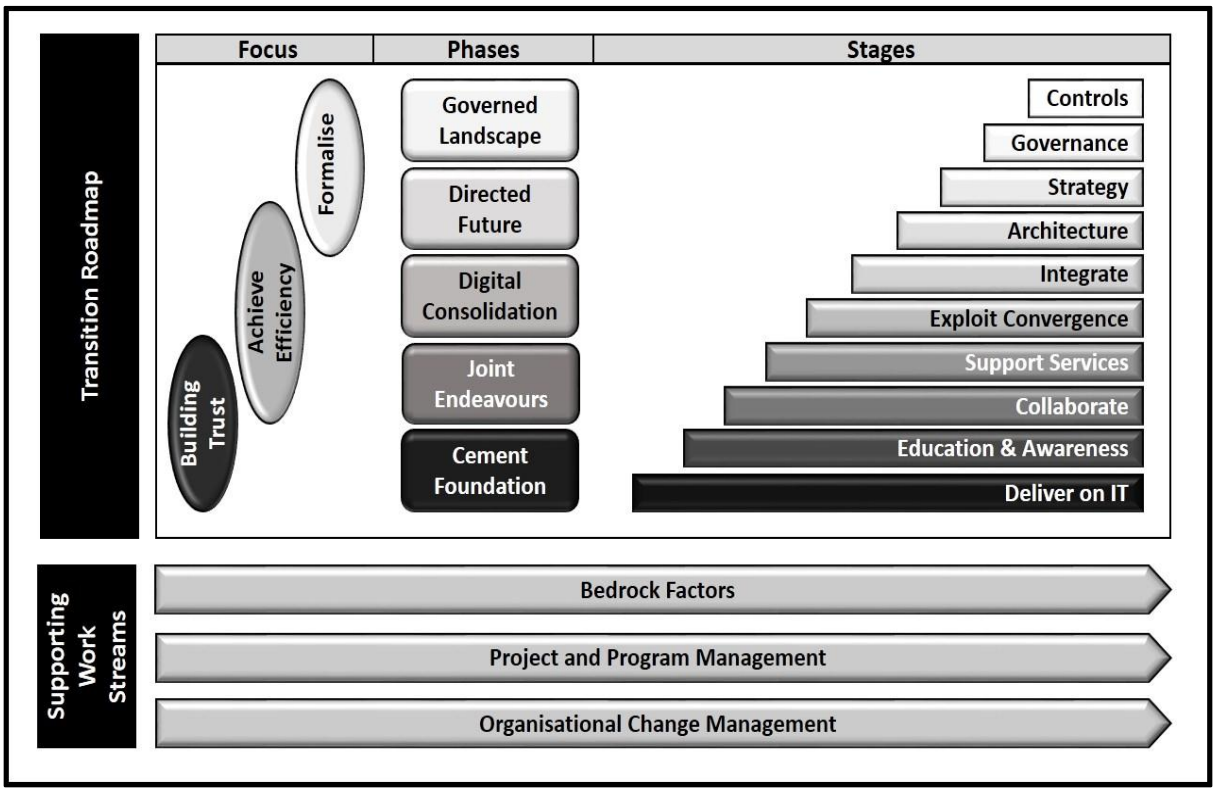


Figure 5-10 Transition Management Constituent Part

The roadmap includes characteristics of a ***maturity model*** for asset information management and digital governance in support of infrastructure asset management *(Wendler, 2012).* The phases and stages of the roadmap represents the improvements, or levels of maturity, of the developmental path over time, from an ad-hoc scenario to a formalised scenario (*Wendler, 2012*). The vision, as defined by the underlying philosophy and principles of the Rand Water

Way, represents the target maturity or "prefect state" of the transition journey *(Becker, Knackstedt & Pöppelbuß, 2009).* The roadmap does not propose a "step ladder" approach to maturity improvement *(Wendler, 2012).* The stages are continuous in nature and each stage provides the foundation for the next stage along the transition journey *(Kaplan & Norton, 2001).* The roadmap can also be used to: 1) determine the current position of the organisation on the "maturity model"; 2) assess its readiness to increase the maturity; and 3) identify the work still to be performed to achieve the target state *(Becker, Knackstedt & Pöppelbuß, 2009).*

The transition roadmap also encapsulates some ***elements of organisation change management***. The focus is first placed on building trust between the digital functions of the organisation before requiring any further involvement from the other digital functions in the transition efforts *(Nfuka & Rusu, 2010; Duck, 1998; Hadaya & Cassive, 2012).* The focus then moves to illustrating and delivering efficiency related value through the sharing of skills and resources, as well as the standardisation, integration and consolidation of the digital infrastructure, processes and asset information *(ISO, 2014; Šaša & Krisper, 2011; Soloman, 2010; von Petersdorff, 2013).* Finally, the focus moves to formalisation, in order to address digital risks associated with digital system integration and digital technology convergence *(The Water Environment Federation, 2010; Anwar & Mahmood, 2014).* This is achieved by addressing: 1) the combined future of the digital functions and landscape; 2) the governance of the digital landscape; and 3) the institutionalisation of the change *(The Open Group, 2009; Wang & Shuo, 2013; Kotter, 1998).*

The ***phases of the roadmap*** are described as follows:

Phases		Description
1	**Cement foundation**	**Purpose:** Provide a solid foundation for the future change efforts by: 1) delivering a quality IT / digital service to the rest of the organisation, including to the other digital functions; and 2) communicating to and educating the other digital functions, in terms of digital service delivery, efficiency improvement opportunities, and risk to the digital environment. **Stages:** 1) Deliver on IT; and 2) Education and awareness. **Outcome:** 1) Improved legitimacy and credibility of the vision and the digital function leading the transition; 2) improved trust between digital functions; 3) improved knowledge of opportunities and risks; 4) increased willingness of the digital functions to participate in the transition; and 5) an increased sense of urgency to change *(Nfuka & Rusu, 2010; Kotter & Schlesinger, 2008; McDowall, 2012).*

	Phases	Description
2	**Joint endeavours**	**Purpose:** Embark on joint ventures between the digital functions within the organisation focusing on common problems, or objectives, as well as the provisioning of shared services related to converged digital technology, where feasible and required. It also attempts to further improve trust between the digital functions via collaboration. **Stages:** 1) Collaboration; and 2) Support services. **Outcome:** 1) Efficient utilisation of digital skills and resources; 2) improved level of trust between and commitment of digital functions; and 3) improved collaboration and cooperation *(Soloman; 2010; Jaatun, Røstum, Peterson & Ugarelli, 2014; Flores, Antonsen & Ekstedt, 2014).*
3	**Digital consolidation**	**Purpose:** Consolidate the digital landscape of the organisation by exploiting the convergence in digital technology and by integrating the digital technology, digital systems and asset information. This is a key requirement and enabler of infrastructure asset management decision making. **Stages:** 1) Exploit convergence; and 2) Integrate. **Outcome:** 1) Consolidated, cost effective and simplified digital landscape; 2) integrated digital landscape and asset information; and 3) improved commitment from digital functions *(Chang, Kauffman & Kwon, 2014; Soloman, 2010; ISO, 2014; Lloyd, 2012).*
4	**Directed future**	**Purpose:** Define, agree and formalise the joint "as-is" and "to-be" enterprise architecture, digital standards and digital strategy(ies) that all digital functions must comply with. **Stages:** 1) Architecture; and 2) Strategy. **Outcome:** 1) Reduced digital landscape risk (e.g. big data, digital technology size and complexity); 2) strategic and architectural alignment; 3) management of asset information as a strategic resource; and 4) formalised commitment and buy-in *(The Open Group, 2009; Lehman & Heagy, 2014; Silva, de Gusmão, Poleto, e Silva & Costa, 2014; Šaša & Krisper, 2011).*
5	**Governed landscape**	**Purpose:** Define, agree and implement formal enterprise-wide digital governance mechanisms and internal operational process controls that all digital functions and solutions must comply with. The prioritisation of the implementation of the controls is risk-based. **Stages:** 1) Governance; and 2) Controls. **Outcome:** 1) Further reduced digital landscape risk (e.g. information security, uncontrolled changes, unclear accountability); 2) improved formalised commitment; and 3) institutionalised change *(Benaroch, Chernobai & Goldstein, 2012; IT Governance Institute, 2012; Kluth, Jäger, Schatz & Baurenhansl, 2014; Kotter, 1998; Anwar & Mahmood, 2014).*

Table 5-11 Transition Roadmap Phases

The transition roadmap is consistent with reflexive, adaptive management as this longer term transition journey is not always a simple straight line *(McDowall, 2012).* There is adequate flexibility within the roadmap to make the necessary "course corrections", whilst still retaining

the overall vision *(Anderson & Anderson, 2001).* This flexibility is built into the roadmap in order to cater for: 1) some degree of uncertainty about the future state; 2) responsiveness to new opportunities, lessons learnt and changes in the environment; and 3) contextualisation of the roadmap to be suitable for any infrastructure asset intensive organisation *(Anderson & Anderson, 2001; McDowall, 2012).* A more detailed description of the phases and stages, as well as additional characteristics of the transition roadmap are provided in ***Annexure A.***

Each of the three ***supporting work streams*** required by the transition roadmap to be successful, will be described. These are the: 1) bedrock factors; 2) project and program management; and 3) organisational change management.

Bedrock factors are those practices that must be in place before the implementation of the transition roadmap. If the transition is proposed by one of the digital functions of the organisation (e.g. corporate IT function), then that digital function must "walk the talk" *(Kotter, 1995 & 1998).* This is achieved by ensuring that all the improvements and practices, demanded from the other digital functions during the transition roadmap, are operational within the environment of the digital function proposing the transition, before demanding that any of the other digital functions implement these practices. It includes the required governance mechanisms, digital systems integration, operational process controls, information management practices and enterprise architecture practices. The existence of these bedrock factors, or practices, will: 1) ensure that the digital function proposing the transition has the necessary credibility and legitimacy to do so; and 2) will prove that the proposed future state is plausible *(Strebel, 1998; McDowall, 2012).* It will further assist in reducing cynicism and suspicion towards the transition initiative by increasing the predictability and understanding of the proposed change and target state *(Duck, 1998; Strebel 1998; Augustine, 1998).*

The implementation of a new way of working includes a ***project and program management*** work stream, in order to: 1) direct, govern and manage the transition; 2) ensure that all individual projects are coordinated and leading the organisation in the same direction towards the agreed vision; 3) ensure that projects are aligned to enterprise-wide governance and risk management directives; and 4) ensure that the program achieve its expected objectives and benefits *(Kaplan & Norton, 2001; PMI, 2013; Kotter, 1995 & 1998).* The transition roadmap is a medium to long term journey and consists of a number of related projects, and some ongoing work that will deliver incremental changes and benefits as part of the overall roadmap *(PMI, 2013; Ross, 2004; Kluth, Jäger, Schatz & Baurenhansl, 2014).*

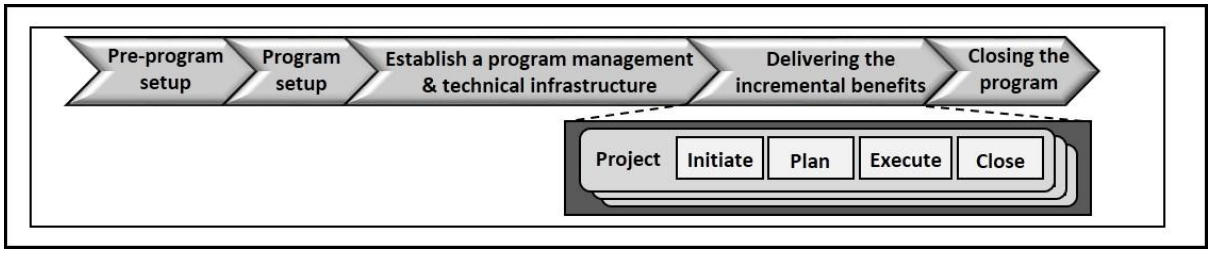


Figure 5-11 Rand Water Project and Program Management Work Stream

This work stream primarily addresses the "hard" or mechanical side of transition and organisational change management, including: 1) frequent progress updates against milestones and targets of the roadmap; 2) commitment of top management; 3) an effective methodology; and 4) the required capacity and resources for the change initiative to be successful *(Sirkin, Keenan & Jackson, 2005; East, 2011; McDowall, 2012; Manganelli & Klein, 1994).* The project and program management work stream represents the way of controlling the work to be performed during the transition.

Organisational change management is an important dimension of the Rand Water Way. The implementation of the Rand Water Way is not a technical project, but is primarily a change project *(Kaplan & Norton, 2001).* It includes integrating formally autonomous, or semi-autonomous, digital functions and / or business units (*Strebel, 1998; Soloman, 2010).* This in turn requires a change in terms of asset information management and digital governance across the organisation *(Lloyd, 2012; Bowen, Chung & Rohde, 2007).* It includes changes to, or standardisation of, processes, roles and responsibilities, as well as decision making authority *(Ross, 2004; IT Governance Institute, 2012).* These previously isolated digital functions are required to spend significant time and money to conform to new enterprise-wide policies, processes, architectures and standards *(Lloyd, 2012; Martin, 1998; Fonstad & Robertson, 2004).* They are also required to work together across functional boundaries, notwithstanding the sometimes territorial behaviour of such digital functions *(Duck, 1998; Goss, Pascale & Athos, 1998).* The purpose of the organisational change work stream is to address the human or soft factors of transition management that increase resistance to the change in order to preserve the past *(Clarke, 2006; Kotter, 1995 & 1998; East, 2011).* This includes the lack of security or safety, lack of trust or suspicion, cynicism, scepticism and feelings of de-valuation of the digital functions impacted by the change *(Johnson, 2010; Mearns, Whitaker & Flin, 2003).* The people in the digital functions who will implement the change via their collective actions, or who will be impacted by the change, will be engaged in a continual and participative process, in order for the transition to be successful *(Anderson & Anderson, 2001; Augustine,*

1998). This includes people from the different levels of the hierarchical organisation and from the digital functions across the organisation *(Prasad, Heales & Green, 2010; Kaplan & Norton, 2001).* The organisational change management work stream includes the continuous change management efforts for the overall vision-based change, as well as each incremental improvement included in the overall roadmap *(Kluth, Jäger, Schatz & Baurenhansl, 2014; van der Voet; 2014).* This includes creating the correct climate for the overall change, engaging the organisation to change, as well as implementing and sustaining the overall change *(Kotter, 1995 &1998).* It also includes the unfreeze-change-refreeze related activities for the smaller changes within the overall change initiative (*Conger, Spreitzer & Lawler, 1999).*

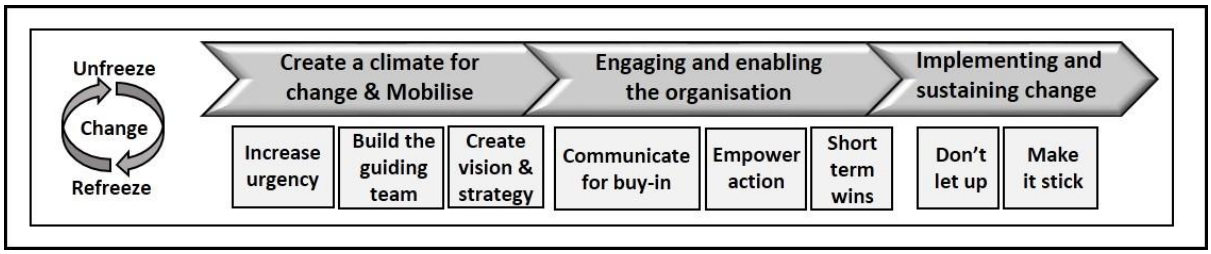


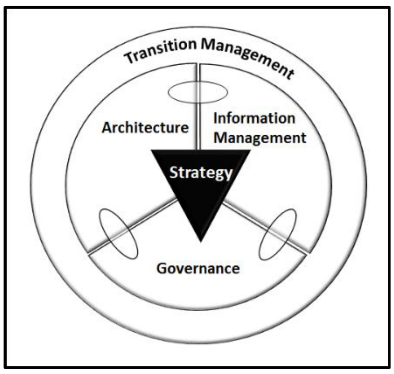
Figure 5-12 Organisational Change Management Work Stream

Organisational change management is not treated as an unrelated or "necessary evil" work stream in the Rand Water Way. In addition to this work stream, organisational change management is explicitly built into the transition roadmap, the bedrock factor work stream and the digital governance framework. The two phases of the roadmap that significantly assist organisational change management, are the Joint Endeavours phase (Deliver on IT; Education and Awareness) and the Cement Foundation phase (Collaboration; Support Services). The focus of these two phases is to build trust in the capability and intention of the digital function proposing the change *(Nfuka & Rusu, 2010; Kotter, 2012).* Provision is made in the digital governance framework for engagement and collaboration (e.g. the digital steering committee and sub-committees) to ensure adequate communication and participation during the transition *(Weill & Ross, 2004; Hadaya & Cassive, 2012; Flores, Antonsen & Ekstedt, 2014).*

Chapter 6 - Instantiation of the Rand Water Way

The purpose of this chapter is to describe the instantiation of the Rand Water Way. It includes a description of the contextualisation of the generalised Rand Water Way based on the characteristic of Rand Water, in order to resolve the related problems. The description is structured according to the constituent parts of the Rand Water Way, namely strategy, architecture, information management, governance and transition management.

6.1. Strategy



The purpose of this section is to describe the instantiation of the strategy constituent part of the Rand Water Way. It describes the formalisation and acceptance of the Rand Water Way as a digital strategy and it describes the primary reasons why Rand Water adopted this strategy.

Rand Water provides an ***essential service*** to a region that generates 60% of South Africa's gross domestic product *(Rand Water, 2013).* Access to clean drinking water is a constitutional right in South Africa. It is enshrined in the Constitution of the Republic of South Africa of 1996. The potable water produced by Rand Water must satisfy the nationally accredited standards on water quality and the World Health Organisation's drinking water quality guidelines. The physical water purification plants of Rand Water are classified as national key points. The security arrangements of these plants must therefore comply with the South African National Key Points Act 201 of 1980. The physical water purification and distribution infrastructure of Rand Water is deemed to be a critical national infrastructure installation. The ***control system functions*** directly support and enable the essential core operations of Rand Water, whilst the IT function focuses primarily on the supporting business processes and decision making. The control systems and instruments are integrated into the converged digital infrastructure and IT systems. They are also integrated into the critical physical infrastructure devices (process device, final control element) that are monitored and/or controlled by the control systems *(The Water Environment Federation, 2007; Soloman, 2010; Hammoudech & Newman, 2013).* Such instruments can therefore impact both the digital technology landscape

and information, as well as the physical infrastructure installation and the core operations of the organisation.

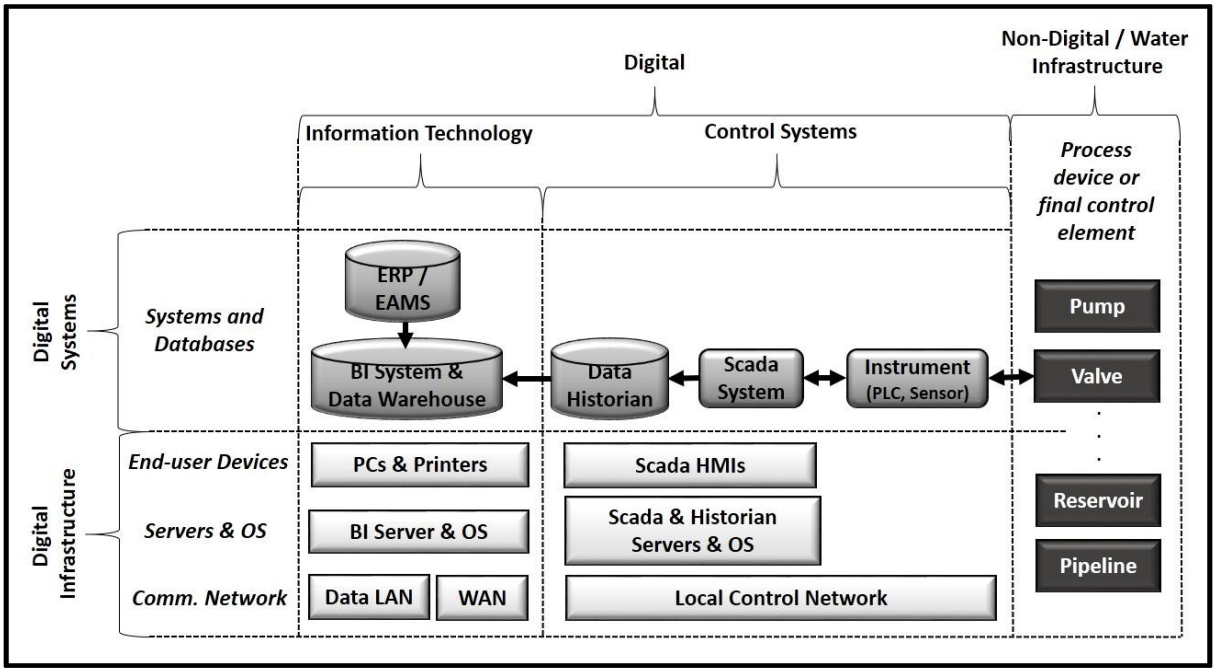


Figure 6-1 Integration of Digital Systems

The ***inherent risk*** to the organisation and its stakeholders associated with the integration of the control systems and related instrumentation into the physical infrastructure installation, is considered to be higher than the inherent risk associated with the integration of the control system and telemetry data into the converged digital infrastructure and IT systems.

The ***responsibility for the essential core operations*** and services of Rand Water resides with the Chief Operating Officer rather than with the Group Shared Services Executive and the Chief Information Officer. This includes the responsibility for the core operations to comply with the relevant legislation and standards. It was therefore decided that the responsibility for the control systems will remain with the Chief Operating Officer, rather than creating a single centralised enterprise-wide digital function reporting to the Chief Information Officer. This will ensure clear responsibility for the essential core business operations and the supporting digital technology.

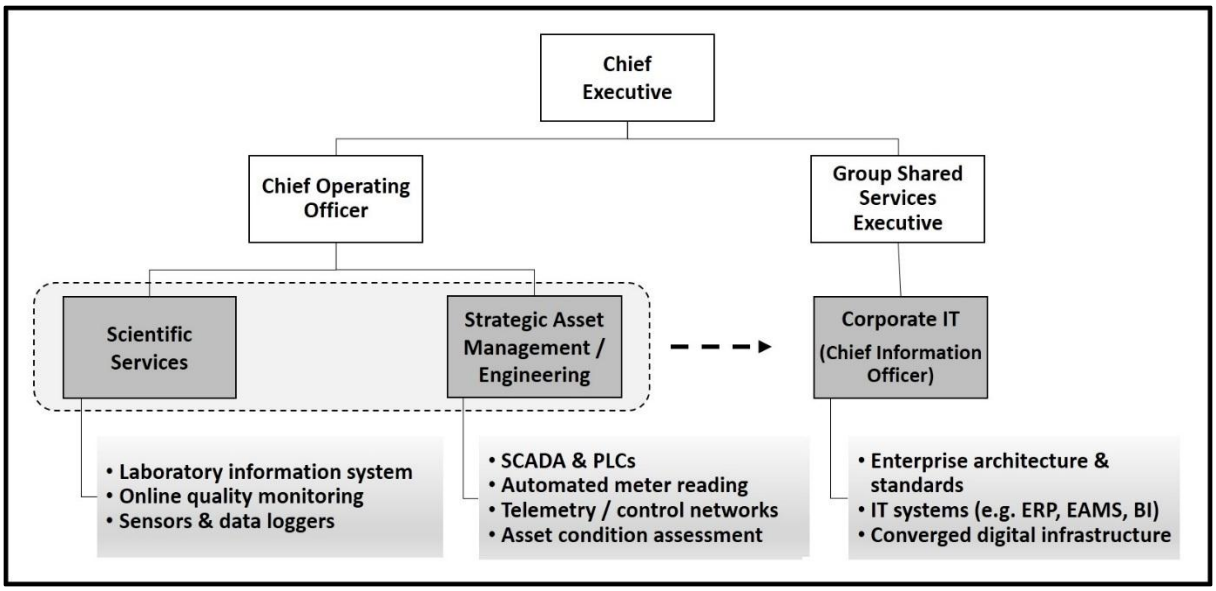


Figure 6-2 Rand Water Digital Organisation

The risk to the overall digital infrastructure and IT systems associated with the convergence in digital technology and the integration of control systems into the IT systems, will therefore have to be addressed via an enterprise-wide digital governance layer spanning across, and applicable to, all three digital functions of Rand Water.

The ***vision of IT at Rand Water*** is to become a trusted business partner that provides a centre of excellence for information and communications technology, business process and information management for the organisation, alongside the convergence and governance of digital technology. The ***mission of the IT function*** is to facilitate and support the achievement of Rand Water's growth strategy through information and communications technology related expertise, innovation, and governance necessary to provide the highest quality of information and communications technology-based services in the most cost-effective manner. The IT strategy is underpinned by the following ***principles*** that are related to, and support, asset information management and digital governance at Rand Water:

Principle	Description
Standardised information access and sharing	The standardisation of information access across the digital systems landscape to ensure the consistent and adequate information security of asset management related data across the systems landscape.
Architecture-centric digital technology	The existence and compliance to an agreed enterprise architecture and standards for all digital functions and solutions across the enterprise, to ensure interoperability.

Principle	Description
Optimised digital infrastructure	Simplifying and optimising the digital infrastructure through standardisation and exploitation of the convergence in digital technology, whilst keeping the operational risk at an acceptable level.
The use of best-fit (fit-for-use) digital technology	The selection and adoption of best-fit technology systems to enable the integration of non-ERP solutions into the digital systems landscape, and the transfer of information between digital systems.
Enterprise-wide digital technology governance	The implementation of, and compliance with, digital governance mechanisms across the enterprise's digital systems landscape and digital functions.

Table 6-1 Rand Water IT Strategy Principles

The ***future states*** defined in the IT strategy that are relevant to, and directly support, asset information management and digital governance in support of infrastructure asset management are:

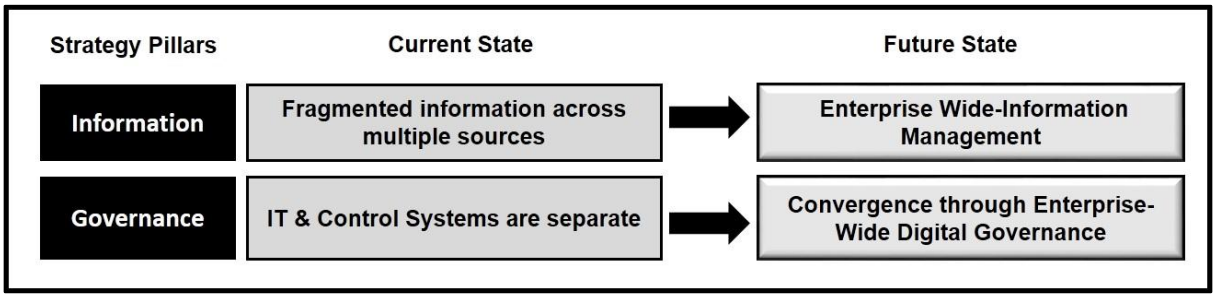
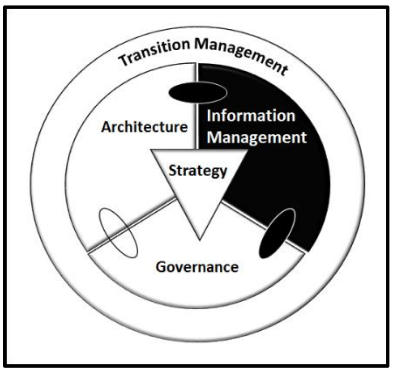


Figure 6-3 Rand Water IT Strategy Future State Extract

Future State	Description
Enterprise-wide digital information management	Moving from a fragmented information landscape managed in isolation by separate digital functions, to managing information as a strategic asset across the enterprise, including asset data from IT and control systems. This will enable asset information from across the digital landscape to be fused and harmonised in support of asset management decision making.
Convergence through enterprise-wide digital governance	Moving from the separation and isolation of IT and control systems to an integrated and governed digital landscape. The benefits and risks associated with the convergence and integration of digital technology, including IT and control systems, will be addressed via enterprise-wide digital governance, instead of centralising the management responsibility of all digital functions into a single organisational unit.

Table 6-2 Rand Water IT Strategy Future State

6.2. Information Management



The purpose of this section is to describe the instantiation of the information management constituent part of the Rand Water Way. It describes the enterprise information management framework of Rand Water, and its key components, in relation to asset information management in support of infrastructure asset management.

An ***Enterprise Information Management Framework*** (EIMF) was defined and implemented for Rand Water that defines how asset information will be managed as an enterprise resource, enabling information exchange and exploitation to support asset management decision making. It is based on the enterprise-wide information management future state, as defined in the Rand Water IT strategy.

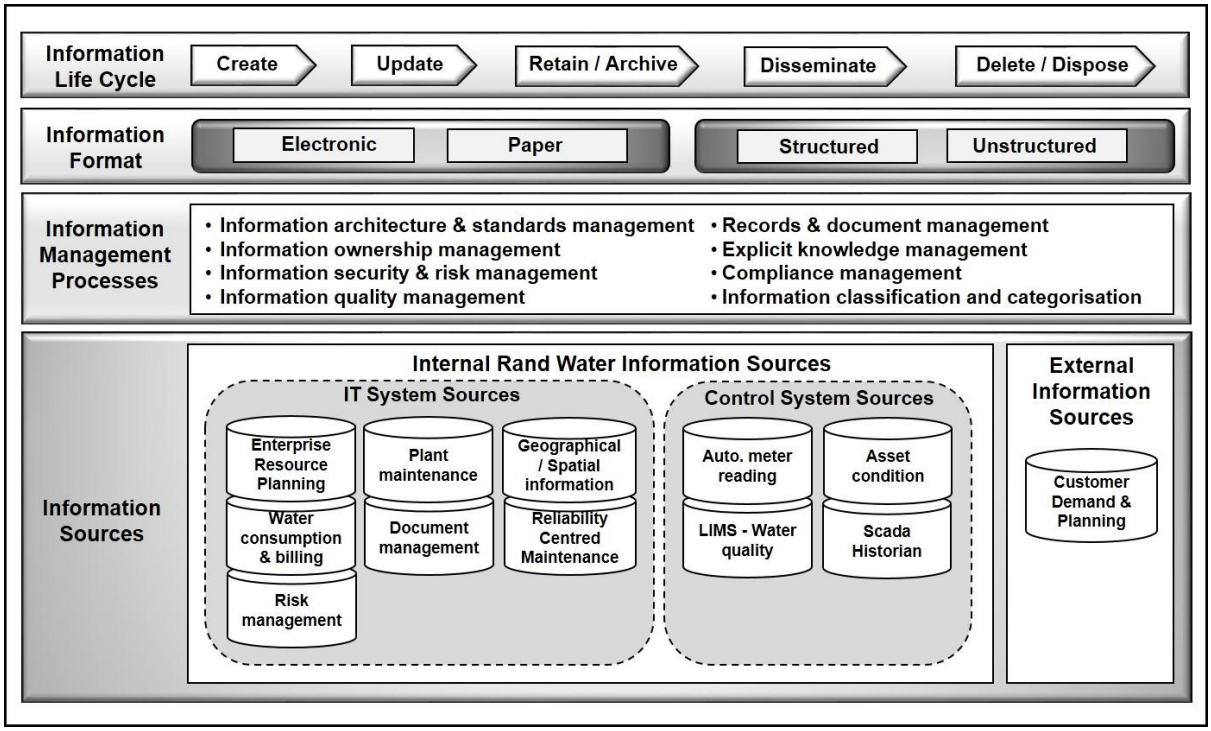
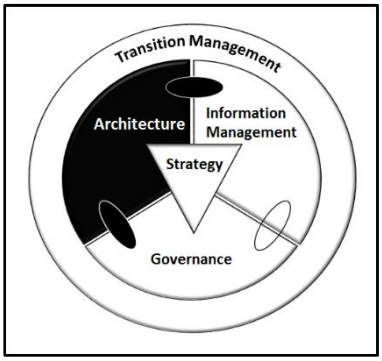


Figure 6-4 Rand Water Enterprise Information Management Framework

The EIMF supplements the Rand Water information architecture by ensuring that asset information, with the appropriate level of quality and value, is made available in a timely manner for evidence-based asset decision making. It addresses the asset information life cycle, asset information format and scope, information management processes, and a catalogue of authentic trusted internal and external asset information sources. Some of the key information

management processes applied to the asset information are: 1) information ownership identification; 2) information security management; and 3) data quality management, including the data consistency and data completeness dimensions of data quality. An EIMF is required at Rand Water to support asset decision making, because the variety and volume characteristics of "big data" are applicable to the asset information of Rand Water. The volume and variety of asset information stored, processed and exploited are increasing exponentially. This is due to: 1) the growth of Rand Water's service footprint; 2) the continued and increasing infrastructure investment; 3) increased emphasis on asset management maturity improvement; 4) increased automation of the core business operations; 5) the use of satellite services to reduce the risk posed by encroachment; and 6) the 25 different asset condition assessment technologies and techniques applied at Rand Water. These digital technologies produce a large amount and wide variety of data, including granular structured data, video, satellite images, radar images, photos, documents and thermal images. The instantiation of the information architecture is described in the next section.

6.3. Architecture



The purpose of this section is to describe the instantiation of the architecture constituent part of the Rand Water Way. It describes the technology view (i.e. network architecture) and the information view (i.e. information architecture) of the Rand Water enterprise architecture, in relation to IT and control systems in support of infrastructure asset management.

An ***enterprise architecture*** was compiled for Rand Water that addresses the IT and control systems of the organisation. It includes the technical architecture, the information architecture, (i.e. application and data architectures) and the information security architecture. It further includes digital standards applicable to the overall digital technology landscape, to ensure digital interoperability.

The ***technology view*** of the enterprise architecture includes the server, storage, end-user devices, network infrastructure, and control system instrumentation. The network architecture for a typical operational site of Rand Water is as follows:

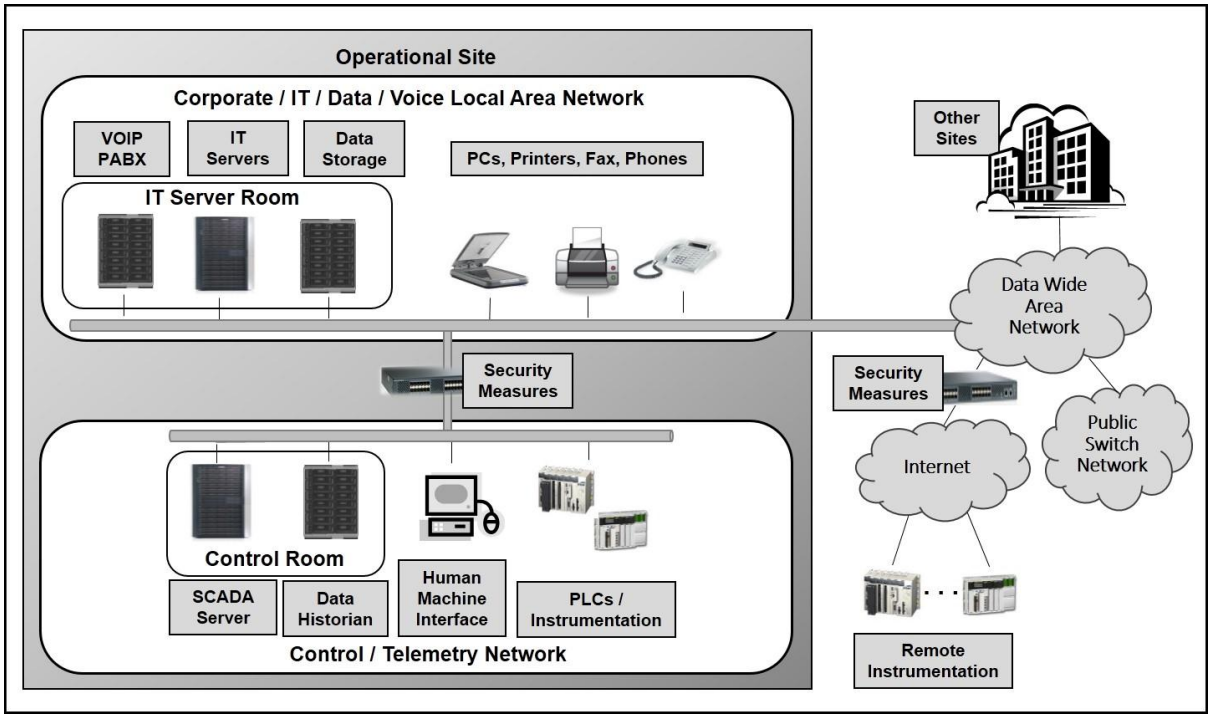


Figure 6-5 Rand Water Network Architecture

Digital network technology convergence was exploited for Rand Water in a way that ensured cost efficiency, whilst keeping the residual risk for the IT environment, control system environment and the physical infrastructure installation, to an acceptable level. The convergence in digital technology was exploited for: 1) the data, telemetry and voice traffic over the wide area network; 2) part of the local area network at each operational site; and 3) connecting remote control system instrumentation via the internet. This resulted in an annual saving of approximately ZAR 10 million. However, the control (telemetry) network at the infrastructure installation level, was retained as a dedicated network. The inclusion of this network into a converged local area digital network, will increase the risk to Rand Water's infrastructure installation to an unacceptable level. The two local area networks (i.e. Corporate / IT and control networks) are linked, in order to allow and enable the flow of asset management related information from the control system instruments to the IT systems. This enables asset information from the control systems and IT systems to be fused and utilised by Rand Water for asset decision making. The inherent risk caused by this integration and convergence, including the security and plant availability risks, are mitigated to an acceptable level by the information security measures implemented at Rand Water. This includes: 1) separating the

hosting of the control system and IT system digital infrastructure at the site to improve physical security; 2) logically separating the data, voice and telemetry network traffic over the physical converged wide area network; 3) linking all control system devices to the dedicated control network, rather than the converged local area network; and 4) logical information security measures. The information security measures were applied across the converged digital infrastructure, between the various Rand Water networks, and at the entry points into the Rand Water network, in order to regulate access to and the flow of information. These security measures ensure that the overall digital landscape is adequately protected from cyber security threats, attacking and exploiting the "weakest link" of Rand Water's large distributed SCADA systems. It will also ensure clarity in terms of the responsibility of the Rand Water digital functions for the digital infrastructure at the site.

Rand Water's ***information view*** of its enterprise architecture is based on the enterprise-wide information management future state, as defined in its IT strategy. The information architecture identifies and defines the complete digital system and database landscape that enables Rand Water to collect, retain, analyse, transform, disseminate, dispose and exploit asset information. It enables enterprise-wide asset information management by ensuring that: 1) the wealth of asset information stored and processed by digital systems is accessible to users and other digital systems; 2) the knowledge of the asset information and the relationship between information elements is improved; 3) asset information across the organisation is unified through consistent semantics, terminology and information definitions, independent of the source of the information; and 4) asset information is captured, or automatically collected, once-off and is re-used, rather than being recaptured in other digital systems. The Rand Water information architecture consists of three layers, namely: the information generation and processing, information exchange, and information exploitation layers. The control systems and databases are included in the information generation and processing layer to supplement the asset information generated by the IT systems. The control system instrumentation that generates, or acquire, the majority of the control system information, is also included in the information generation and processing layer of the Rand Water information architecture. The information exploitation layer consists of longer term data storage and business intelligence solutions. It exploits harmonised and fused asset information from all trusted digital data sources for asset decision making.

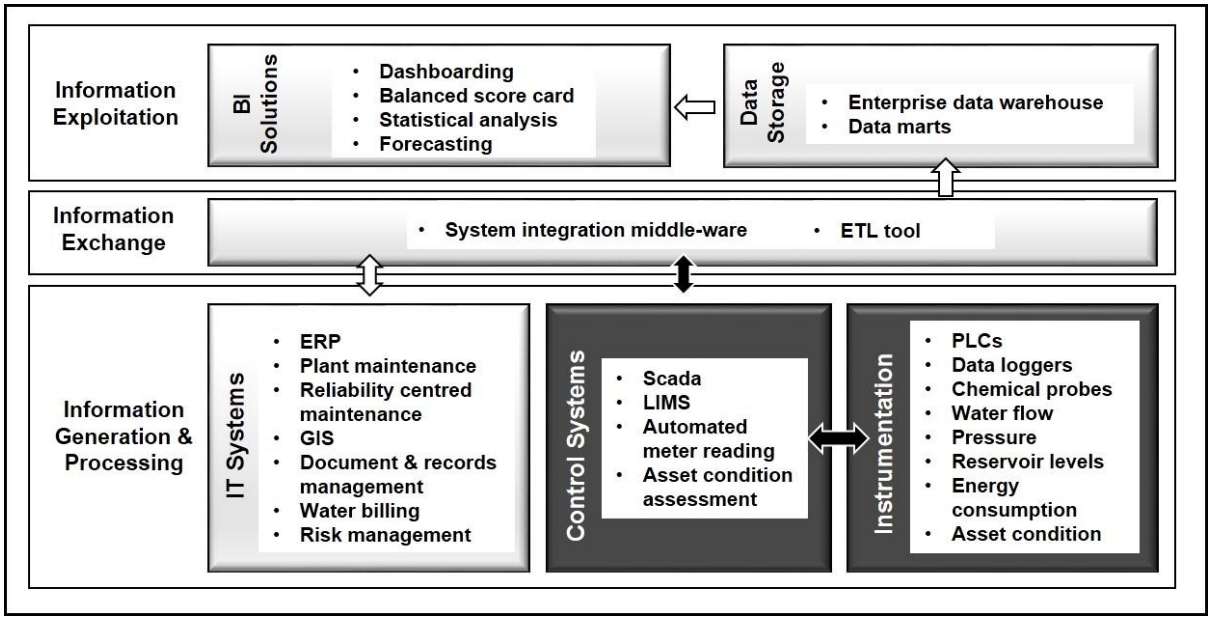
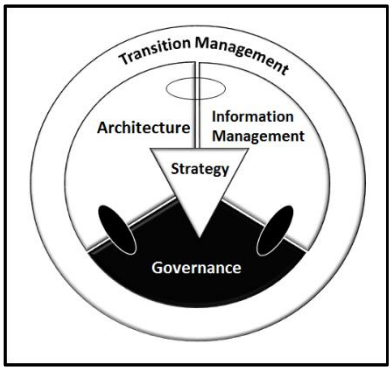


Figure 6-6 Rand Water Information Architecture

The information exchange layer consists of middleware, as well as extract, load and transform (ELT) tools. It exchanges the required information between digital systems for further processing (e.g. volume meter readings for customer water consumption and billing), retention, compliance and asset decision making purposes.

6.4. Governance



The purpose of this section is to describe the instantiation of the governance constituent part of the Rand Water Way. It describes the digital governance framework, as well as the risk-based selection and prioritisation of the governance level mechanisms and operational process controls within the context of Rand Water. It further illustrates the implementation of one of the digital operational process controls.

Rand Water opted to comply with the King III Code of Good Governance for South Africa (aka King III Code) *(Rand Water, 2014).* The King III Code and other related literature state that the organisation's board is accountable for IT governance, and that the IT governance framework must be integrated into the existing larger corporate governance framework *(Institute of Directors of South Africa, 2009; Weill & Ross, 2004).* To this end a Rand Water ***digital governance framework*** was developed, approved and implemented. It includes all the Rand Water corporate governance structures with any digital governance related accountability

or responsibility. It further includes the board, executive management and operational levels of the organisation.

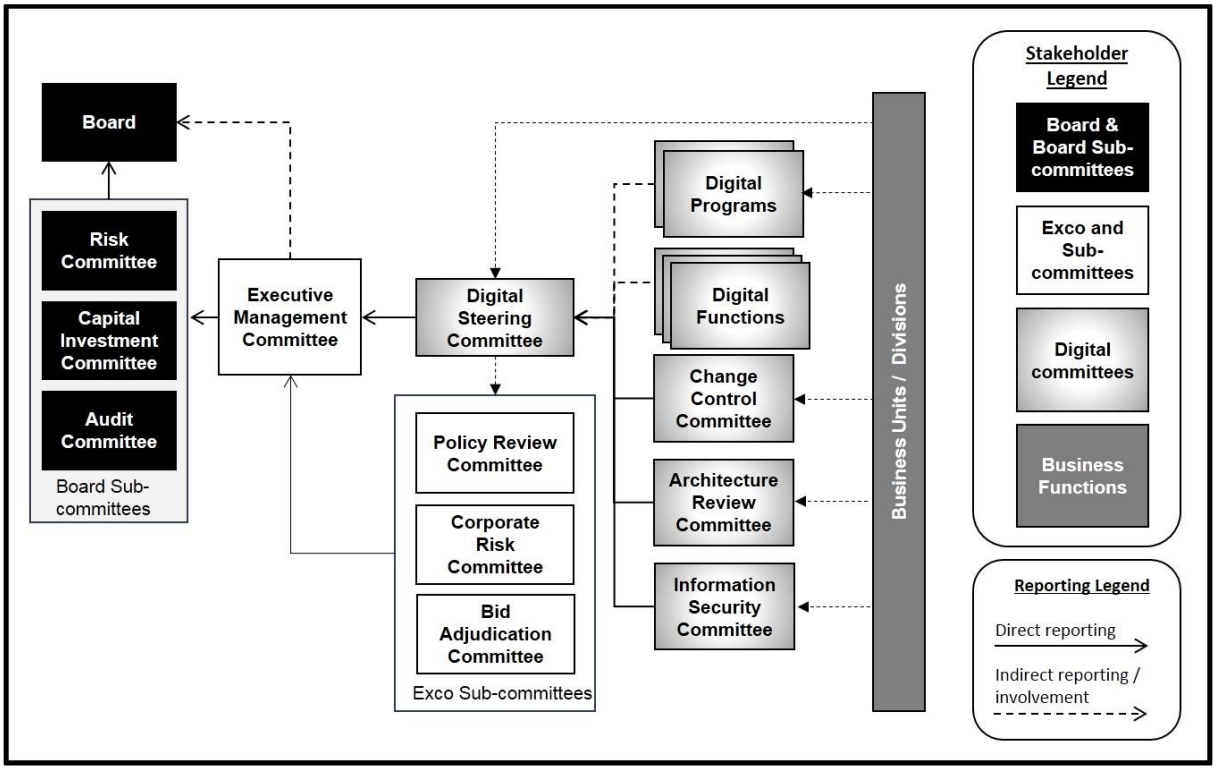


Figure 6-7 Rand Water Digital Governance Structures

The governance structures include the board, sub-committees of the board, the executive management committee and the sub-committees of the executive management committee. The three board sub-committees with digital governance-related accountability are: 1) the risk committee focusing on digital risk and digital governance; 2) the audit committee focusing on independent assurance and the digital landscape relating to financial reporting; and 3) the capital investment committee focusing on digital capital investments and value delivery. The three sub-committees of the executive management committee with digital governance-related responsibilities are: 1) the policy review committee focusing on all Rand Water policies, including digital policies; 2) the corporate risks committee focusing on strategic risks, including digital risks; and 3) the bid adjudication committee focusing on the procurement of products and services, including digital products and services. At the centre of the framework is a single enterprise-wide digital steering committee. It was declared a sub-committee of the executive management committee of Rand Water. The digital steering committee is supported by operational structures focusing on the three digital functions within the organisation, key digital programs, and key digital governance mechanisms (i.e. digital architecture and

standards, information security and change control). The roles and responsibilities of the digital steering committee and its sub-committees are as follows:

Structure	Roles and Responsibilities Summary
Digital steering committee	Ensures that: 1) enterprise-wide digital governance is defined, implemented and operated effectively within Rand Water; 2) there are enterprise-wide agreed digital strategies, architectures, frameworks, policies, processes, procedures, structures and standards; 3) Rand Water has an end-to-end integrated digital environment, including digital infrastructure, systems and digital information; and 4) knowledge sharing, resource sharing, collaboration, service delivery, and change management are effective within the Rand Water digital environment.
Architecture review committee	Ensures that: 1) Rand Water has an end-to-end coordinated, cost effective, agile and low risk enterprise architecture, standards and digital landscape; and 2) new digital solutions comply with the Rand Water enterprise architecture and standards.
Change control committee	Ensures that: 1) changes to the digital production environment of Rand Water are managed and executed in a controlled manner; and 2) the risk associated with uncontrolled changes to the production environment is adequately mitigated.
Information security committee	Ensures that the digital technology landscape and digital information is adequately protected in terms of availability, integrity and confidentiality.

Table 6-3 Rand Water Digital Governance Structure Roles

The Rand Water digital governance framework is supplemented by a digital governance charter, responsibility-assignment matrix (aka RACI matrix) for key decisions, a combined assurance model, terms of references for each of the decision making structures, and governance processes (e.g. Ensure IT governance, Ensure value delivery). This ensures that: 1) the direction provided by the board and executive management is operationalised and embedded within all the digital functions of Rand Water; 2) that transparency is increased and adequate assurance is provided to the board; and 3) that the digital governance roles, responsibilities and decision making authority of the three digital functions are clearly defined and agreed to. Rand Water also needs to comply with the Department of Public Services and Administration Corporate Governance of ICT Framework (DPSA CGITF), as approved by the Cabinet of South Africa *(Department of Public Service and Administration, 2012).* The role of the Rand Water Chief Information Officer (General Manager IT) fulfils the role of the Governance Champion in relation to the corporate governance of ICT, as required by this framework. This role is responsible for ensuring that the corporate governance of digital technology is implemented, maintained and executed in the organisation.

The IT governance and operational process controls, to be extended to the control system functions, were ***prioritised.*** Control systems are not explicitly specified in the King III Code or the DPSA corporate governance framework *(Institute of Directors of South Africa, 2009; Department of Public Service and Administration, 2012).* Extending IT governance mechanisms to the control system environment therefore needs to deliver value to the organisation beyond compliance to any standard, code or framework *(Raval & Dyche, 2012; Pilling, 2010).* It should adequately mitigate the risk related to digital technology convergence and the integration of IT and control systems *(Port & Wilf, 2014; Webb, Ahmad, Maynard & Shanks, 2014).* The skill required to design, implement and maintain the control systems is considered to be a scarce and critical skill at Rand Water. The control systems should be available on a 24/7 basis, in order to support the essential core business operations of Rand Water. The portfolio of digital governance mechanisms and operational process controls should therefore avoid the consequences of over-regulation *(Verhoef, 2007).* Examples of these potential consequences are: 1) increased cost without adding additional value: and 2) a negative impact on productivity that results in inefficient service delivery by control system functions to the core business of Rand Water. The appropriate, or "just enough", governance mechanisms and operational process controls are required for the Rand Water environment, in order to achieve a balance between cost, value and risk.

A risk assessment was performed in order to identify and prioritise the digital governance mechanisms and operational process controls, required to adequately mitigate the asset management decision support and digital landscape risks, as defined in chapter 5. The risk-based prioritisation approach ensures that limited and scarce Rand Water control system resources and expertise are being effectively utilised, whilst at the same time protecting the high value and most critical asset information and related digital technology from high-risk scenarios. It further ensures that the portfolio of prioritised governance mechanisms and operational process controls is not a "one size fits all" solution, but is tailored for Rand Water, based on the characteristics of the organisation.

The results of the risk assessment and the identification of risk mitigating measures are as follows:

Governance and Management Levels Risks and Mitigation Measures			Typical / Primary Root Causes								
			Information security threats	Uncontrolled changes to digital landscape	Natural and other disasters	Inadequate asset data quality	Lack of digital system interoperability and integration	Increased digital technology regulation and non-compliance	Lack of digital risk management	Digital function longer term misalignment	Lack of digital policies, processes & procedures
Digital Risks	Decision Support Risk		●	○	○	●	●	○	○	●	●
	Digital Landscape Risk		●	●	●			●	●	○	●
Risk Mitigation Measures	Governance Mechanisms	Digital policies	●	●	●	●	●	●	●	○	●
		Digital governance framework	●	●	●	●	●	●	●	○	●
		Digital compliance framework	○	○	○	○	○	●	○	○	●
		Digital strategy(ies) & alignment	○	○	○	○	●	○	●	●	○
		Digital process control framework	●	●	●	●	●	○	●	○	●
		Digital risk management framework	○	○	●	○	○	○	●	○	○
	Operational / Management Controls	Architecture & standards management	○	○		●	●			●	○
		Enterprise information management	●			●	●	○	○		●
		Logical information security management	●	○	○	●	○	○	○		○
		Business continuity management	○	○	●	○			●		●
		Operational risk management	●	●	●	●		●	●		●
		Change and configuration management	○	●		○	○				●

Legend: ● *Significant / high / direct contribution* ○ *Medium / minor / indirect contribution*

Figure 6-8 Rand Water Control Prioritisation Risk Assessment

The ***primary root causes*** that contribute significantly towards either, or both, of the two risks at Rand Water are:

Root Cause Name	Description
Information security threats	Increased information security threats and the lack of adequate logical information security counter measures, such as information access control and protection measures.
Uncontrolled changes	Uncontrolled changes to the digital landscape, due to the lack of change and configuration management measures applied to all Rand Water's digital technology solutions.
Disasters	Natural and other disasters and the lack of adequate and tested digital technology business continuity and disaster recovery measures.
Inadequate data quality	Inadequate data quality (completeness / correctness), due to the lack of adequate data quality measures and clear information ownership across all asset data sources.

Root Cause Name	Description
Lack of digital interoperability and integration	Lack of digital technology interoperability and integration, due to the absence of complete and agreed upon digital architecture and standards or non-compliance by Rand Water digital functions with the digital architecture and standards.
Increased relevant regulations	Increased digital technology related regulations, such as legislation, standards, frameworks and codes, as well as non-compliance thereto.
Lack of risk management	Lack of effective risk management within and across the Rand Water digital functions at both an operational and strategic / corporate level.
Digital function longer term misalignment	Misalignment between the three digital functions of Rand Water, in terms of longer term strategy, direction and the future state architecture.
Lack of digital technology directives	Non-existing, inadequate or out of date internal digital technology directives, such as policies, processes and procedures, or non-compliance by Rand Water's digital functions and projects thereto.

Table 6-4 Rand Water Digital Risk Root Causes

Those governance mechanisms and operational process controls that make a direct contribution towards the resolution of these root causes are considered as essential, and the remainder are considered as important. The risk assessment showed that each of the high level governance mechanisms address all the root causes at least indirectly, whilst the operational process controls are more focused in terms of addressing specific root causes. The governance mechanisms and operational process level controls were unpacked and further analysed.

The following digital ***governance mechanisms*** are considered as relevant and were categorised according to their level of criticality, based on the result of the risk assessment and analysis:

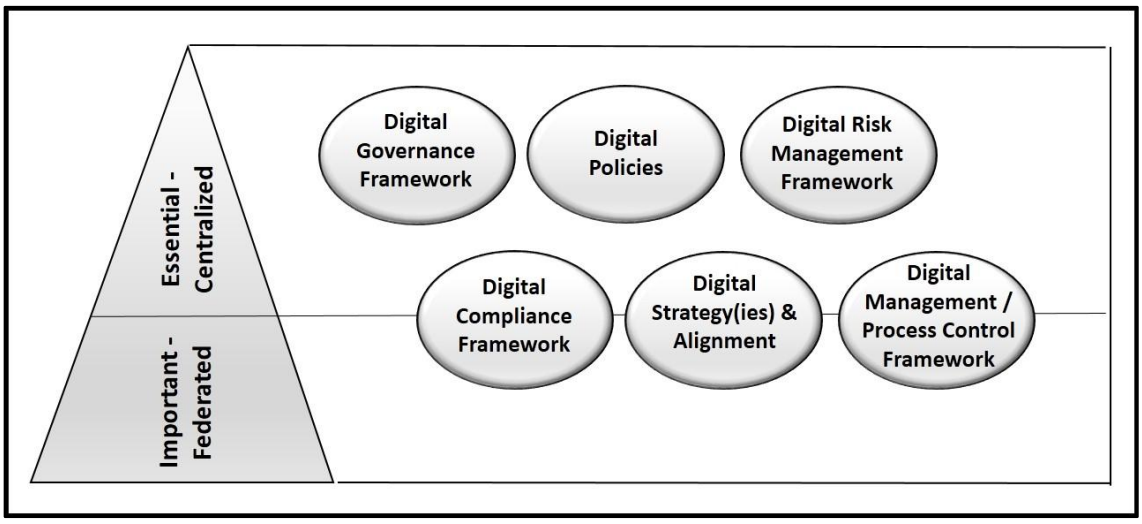


Figure 6-9 Digital Governance Mechanism Criticality Categorisation

The level of criticality of these governance mechanisms and the reason for the categorisation are as follows:

Governance Mechanism	Description
Digital governance framework	The digital governance framework, including all its constituent parts, is considered to be essential for Rand Water. It has a direct and significant impact on the majority of root causes. The constituent parts of the framework include the digital governance principles, structures, charter, responsibility-assignment matrix and governance processes. This framework will be a single centralised enterprise-wide framework applicable to all Rand Water digital functions, solutions and asset information sources.
Digital policies	A single collection of digital policies is considered as essential for Rand Water. The digital policies have a direct and significant impact on the majority of root causes. These policies apply to all the digital functions of Rand Water and must be complied with. It will also be utilised to direct and govern those non-essential operational processes and associated process controls that are defined, implemented and executed on a federated basis by the three Rand Water digital functions.
Digital compliance framework	A compliance framework, consisting primarily of a compliance checklist and a compliance process, is considered essential. A single enterprise-wide digital compliance framework was defined, approved and implemented. This includes all digital related legislation, standards, codes and frameworks that must be complied with by Rand Water. The independent assessments that must be performed to produce the required evidence of compliance, can be executed on a federated basis by each of the digital functions of Rand Water.
Digital strategy and alignment	Digital strategies and strategy alignment is primarily considered to be essential. This is limited to those strategies that direct the overall digital landscape or are associated with the two primary risks of this research topic (e.g. digital governance, digital security, digital architecture and standards). Strategic themes and principles that are not associated with the two primary risks, are considered to be non-essential (e.g. Green IT strategy).
Digital risk management framework	A single common risk management framework, as a basis for digital risk management is considered essential, in order to ensure adequate and comparable digital risk management across all the digital functions and solutions. This includes the risk management methodology, risk appetite and risk tolerance levels. The prioritisation of the execution of digital risk management is addressed as part of the management level controls prioritisation and categorisation.
Internal management process / control framework	The selection of a single foundation for the digital operational process control framework for all digital functions is considered to be essential. All operational process controls, whether deemed to be essential or non-essential, must be based on the common foundation framework. The non-essential operational process controls may be defined and implemented on a federated basis by each of the Rand Water digital functions, as long as they utilise the common foundation framework as a basis to ensure a common reference point and a common set of terminology.

Table 6-5 Rand Water Governance Mechanism Categorisation

The following are examples of ***Rand Water characteristics*** that influenced the prioritisation of the governance mechanisms within the context of Rand Water:

Rand Water Characteristic	Description
Corporate mechanisms	Rand Water has a number of corporate governance mechanisms that all functions, including the digital functions, must comply with. This includes an enterprise risk management framework and a corporate governance framework. The digital functions at Rand Water are not treated differently from any other functions and must comply with these corporate governance mechanisms. This increased the need for a single corporate-wide digital response (e.g. digital governance framework).
Generic digital policies	Rand Water opted to keep its digital policies at a generic level. The policies were limited to digital security, acceptable use, information management, service delivery and solution delivery. It excluded unrelated operational regulations, such as the right to use A3 colour printing capabilities. If such operational regulations were included in the collection of digital policies, then some of the digital policies would be considered as non-essential.
Digital strategy and sub-strategies	Rand Water defined a single IT strategy, and a number of sub-strategies, that focus on how the various future states of the overall IT strategy will be achieved. Examples of these include green IT, enterprise-wide digital governance and digital information security strategies. Only some of these sub-strategies are directly related to the two primary risks. It was therefore possible to differentiate between essential and non-essential digital strategies for Rand Water, and strategy alignment at a sub-strategy level.
Internal management / process control framework as guideline	Rand Water adopted COBIT as its single common foundation for all the digital functions, as well as for independent assurance purposes. Rand Water did not elect to comply with COBIT, as specified in the Rand Water digital compliance checklist. Instead, COBIT is considered as a "good practice" guideline and a common set of terminology, which will be used as input when the individual digital functions identify, define, implement and apply their function-specific operational processes and process controls.

Table 6-6 Governance Mechanism – Rand Water Context

The following ***management / operational level process controls*** were categorised according to their level of criticality, based on the result of the risk assessment and analysis:

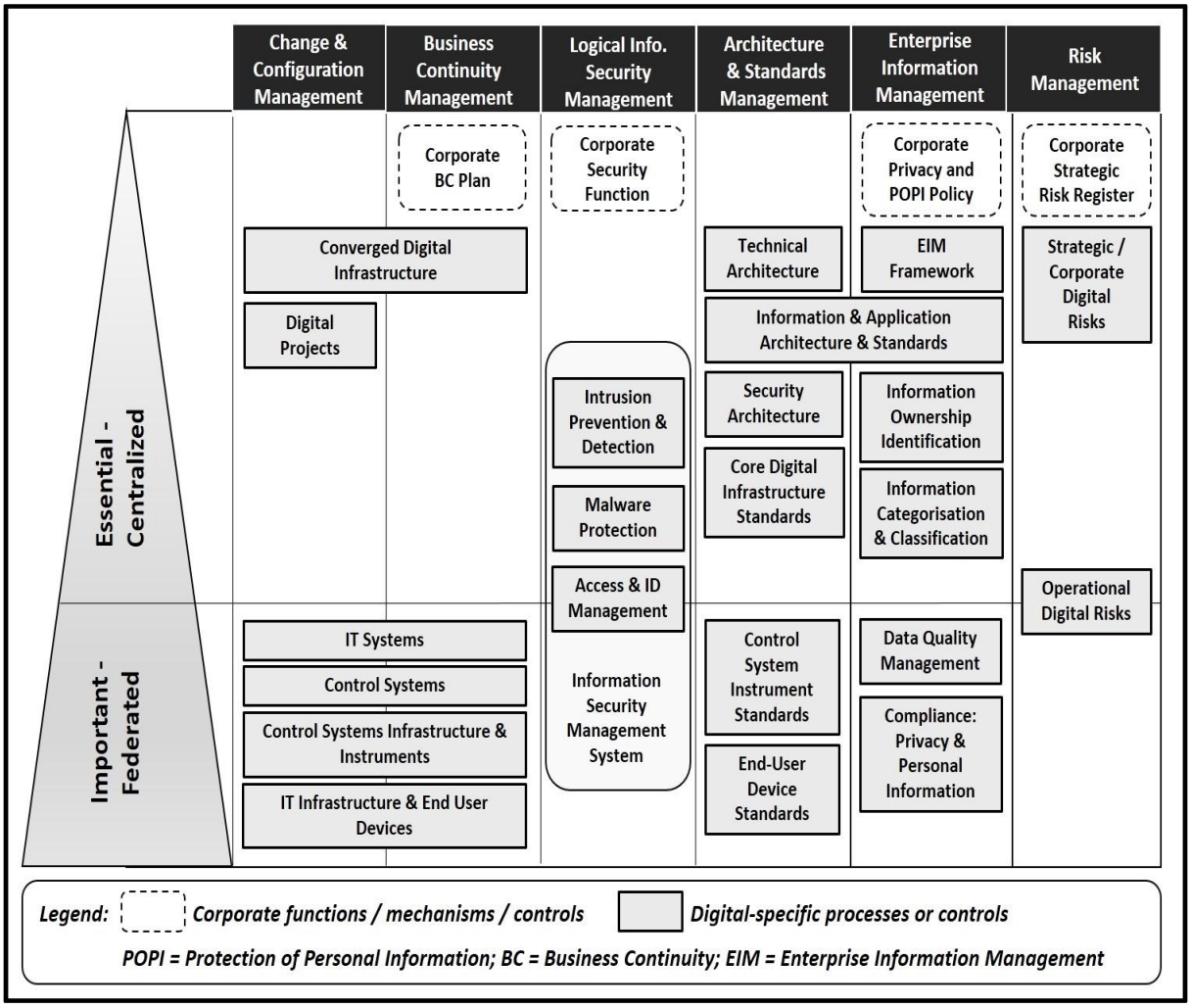


Figure 6-10 Digital Operational Process Controls Criticality Categorisation

The operational process controls are related to the operational digital processes identified as mitigating measures during the risk assessment, namely: change and configuration management, business continuity management, logical information security management, digital architecture and standards management, enterprise information management, and digital risk management. Three of the six operational processes relate to information security, namely: change and configuration management, business continuity management, and logical information security management. Overall, the emphasis is placed on the converged integrated digital infrastructure, digital projects, strategic and common digital risks, logical information security measures, the enterprise information management framework, and the enterprise digital architecture.

The level of criticality of each of the operational process controls is as follows:

Operational Process Controls	Description
Change and configuration management	Change and configuration management for digital projects and the converged digital infrastructure of Rand Water are considered as essential and will be performed in a centralised manner (i.e. one change control committee and one process). Changes to individual systems (IT or control systems), IT specific infrastructure, control system specific infrastructure (e.g. control network), end-user devices and control system instruments are deemed important, but not essential. These controls may be defined, implemented and executed by the three Rand Water digital functions on a federated basis.
Business continuity management	Business continuity, including disaster recovery, of the converged integrated digital infrastructure for all digital systems is considered as essential. A single business continuity and disaster recovery plan is required for the converged integrated core digital technology landscape. Business continuity and disaster recovery plans are also required for IT systems, control systems, end-user devices and dedicated control system infrastructure. These plans are considered to be important and may be defined, implemented and tested by the relevant digital function on a federated basis.
Logical information security management	The logical information security measures that are deemed essential are intrusion protection and malicious software protection. These measures are applied to all digital systems and converged digital devices. They are centralised in the form of a single responsible digital function, a single process and a single set of enabling tools. Access and identity management for the converged network is considered essential and is centralised. Access management to other systems and networks are deemed to be important, and may be performed on a federated basis by the relevant digital function responsible for the digital solution.
Digital architecture and standards management	A single enterprise-wide digital architecture is considered essential for Rand Water to ensure interoperability within the digital landscape. All the Rand Water digital solutions and digital functions must comply with the digital architecture and standards. A common enterprise-wide agreed upon set of standards for asset information and the core digital infrastructure (e.g. converged network, control network, servers, data storage) is essential. The standards for end-user devices and control-system instrumentation are considered to be important. Such standards may be defined and implemented on a federated basis.
Enterprise information management	A single enterprise-wide asset information architecture, enterprise information management framework and a set of asset information standards are considered to be essential. They are managed by a centralised information architecture function. There are two asset information management processes that are deemed to be essential, namely: 1) the identification of information ownership; and 2) the categorisation and classification of information, in terms of sensitivity and personal information. There are two important information management processes, namely: the management of asset data quality, and the management of compliance to regulations in terms of the protection of personal information and privacy. These may be executed on a federated basis by the respective digital functions.

Operational Process Controls	Description
Digital risk management	A single unified response from all digital functions to strategic digital related risks is essential, especially if it relates to and potentially impacts asset information originating from either IT or control systems. This response includes the risk identification, definition and assessment of the risk and existing controls, as well as risk mitigating plans. The management of operational risks is considered to be important and may be managed by the various digital functions on a federated basis. The exception is the management of common operational risks. Such risks must be managed in a centralised manner to avoid duplication and conflict in relation to other essential controls and risk mitigating plans.

Table 6-7 Rand Water Operational Process Controls Categorisation

Digital operational controls do not exist in isolation. They impact one another. One control can reduce the level of criticality of another, if it serves as a compensatory control and risk mitigating measure for the risk associated with the other control. An example of the inter-dependency of operational controls at Rand Water is the existence of logical security controls (e.g. security measures between the converged and control networks) and data exchange "buffers" between control systems and IT systems (e.g. SCADA data historian). These controls reduce the risk to the overall Rand Water digital landscape and asset decision making, caused by uncontrolled changes to digital systems and dedicated plant-level control networks. The risk is reduced to such an extent that the change and configuration management of the digital systems and the plant level control networks, are not considered essential, and may be executed on a federated basis.

A ***combined assurance model*** was defined and implemented for the digital environment. It is based on the corporate combined assurance model of Rand Water and aims to improve transparency and provide assurance to the executive management and the board, regarding the adequacy of the digital controls. This is especially important for the federated controls.

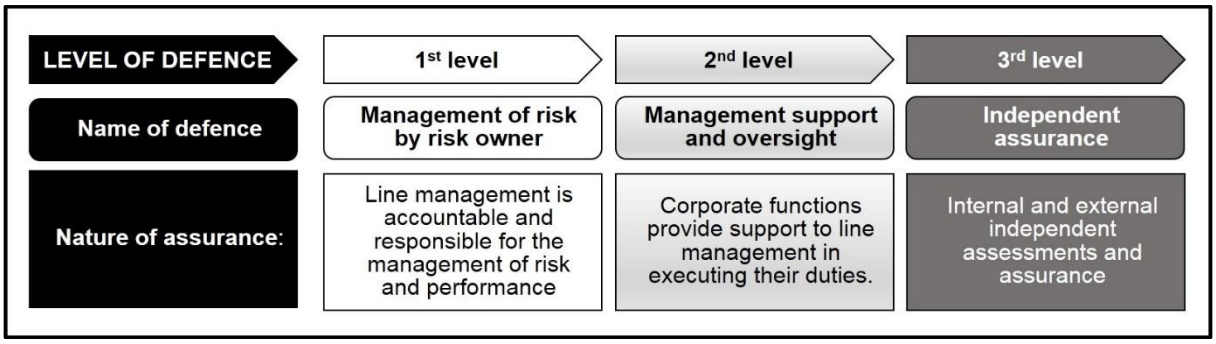


Figure 6-11 Rand Water Digital Combined Assurance Model

The combined assurance model consists of 3 levels of defence, namely: 1) the management of risk by the risk owner; 2) management support and oversight; and 3) independent assurance. The content of these 3 levels of defence is as follows:

Level of defence	Content
1st	**1. Essential centralised digital governance mechanisms:** Digital governance framework and charter; digital compliance framework; digital process control framework; and digital policies defining the rules and principles for all digital functions. **2. Essential / centralised operational process controls:** Architectures & standards; logical security measures; enterprise information management; strategic digital risk management. **3. Digital performance reporting.**
2nd	Corporate frameworks and mechanisms, e.g. enterprise risk management framework and risk register; corporate business continuity framework; corporate quality management; corporate security policy; corporate protection of personal information management policy; and corporate records management framework and policy.
3rd	Internal and external ISO 9001-based quality management audits; external legislative compliance assessments; independent King III and DPSA digital governance framework compliance assessments; and internal audit and external audit performing risk based audits.

Table 6-8 Rand Water Digital Combined Assurance Model

Performance reporting is one of the key assurance mechanisms. It will ensure transparency and should be performed by all three digital functions of Rand Water. The digital functions submit their performance reports to the IT governance structures, such as the digital steering committee. The report(s) should address at least service management and significant investments, as well as governance, risk and compliance related statuses and improvements.

The "change and configuration management" process, as depicted in figure 6.10, will be used as an ***example to illustrate the practical implementation*** of the prioritisation and categorisation of operational process controls at Rand Water. The purpose of this process is to manage, or control, changes to the digital production environment, in order to reduce the risk to the integrated production environment, due to uncontrolled changes. It should not be confused with "organisational change management", as defined in the transition and change management constituent part of the Rand Water Way. There are 2 related centralised governance level mechanisms, namely a digital service delivery policy and the digital process control framework. There are 2 related centralised operational process level controls, namely the management of changes to the converged digital infrastructure and the management of changes

made by digital projects. There are four related federated operational process level controls, namely the management of changes to: 1) IT systems; 2) control systems (e.g. SCADA, LIMS); 3) control system infrastructure and instrumentation (e.g. telemetry network, PLCs, sensors and data loggers); and 4) IT-specific infrastructure and end user equipment.

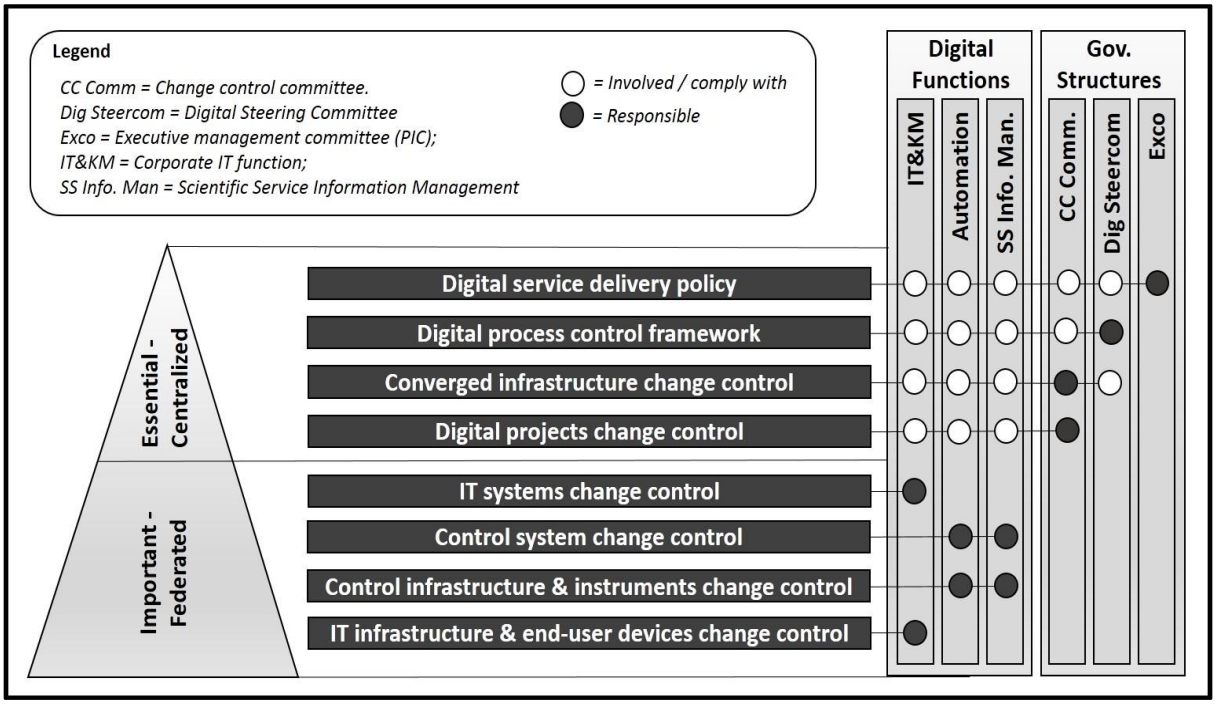


Figure 6-12 Change and Configuration Management - Implementation Illustration

The practical implementation of the "change and configuration management" process in Rand Water is further illustrated as follows:

Control	Description	Roles & Responsibilities
Digital service delivery policy	The single service delivery policy governs and directs the management, or control, of changes to the digital production environment. It provides the rules, standards and principles that all digital functions must comply with, e.g. "*The digital change and configuration management process must ensure that changes are recorded, assessed, reviewed, authorised, tested, implemented, and released in a controlled manner".*	The policy is approved by the executive management committee, as delegated by the board of Rand Water, and as recommended by the digital steering committee. All digital functions, as well as their change and configuration management processes and structures, must comply with the provisions of this policy.

Control	Description	Roles & Responsibilities
Digital process control framework	A common process control framework provides guidance regarding the change and configuration management processes to be defined and executed by the digital functions. A combination of COBIT 5.1 and ITIL is used by Rand Water for this purpose.	The process control framework is selected by the digital steering committee of Rand Water. All digital functions and the centralised change control committee must use this as a foundation for defining their change and configuration management related processes and procedures.
Change to the converged digital infrastructure and changed caused by digital projects	A single change and configuration management process is defined and implemented for managing changes to the integrated converged infrastructure of Rand Water and changes caused by digital projects. The change control committee chairperson reports on a quarterly basis to the digital steering committee regarding its activities, problems and improvements.	This is performed via a single change control committee, which is a sub-committee of the digital steering committee. All digital functions must follow the defined process and must submit intended changes to the change control committee. The digital steering committee defines the terms of reference of, and appoints, the change control committee.
Change to IT systems	A process and structure must be defined for managing changes to the integrated IT systems landscape. This may be separate from the centralised process and change control committee, as long as it complies with the service delivery policy and process control framework. Rand Water opted to combine this with the efforts of the centralised change control committee for efficiency purposes, even though it is not necessary or compulsory.	The IT&KM division (corporate IT function) is responsible for all IT systems at Rand Water. This function is responsible for defining, implementing and executing the change and configuration management processes and structure for IT systems.
Change to control systems, control system infrastructure and instruments	A process and structure must be defined for managing changes to the control systems, the control system infrastructure and the related instrumentation. This may be separate from the centralised process and change control committee, as long as it complies with the service delivery policy and process control framework.	Each of the control system functions is responsible for this within their own area of responsibility. The Automation function is responsible for managing changes to the SCADA system, the control networks at the plant level and the related instrumentation (e.g. PLCs). The Scientific Services Information Management function is responsible for managing changes to the LIMS system and the related instruments.

Control	Description	Roles & Responsibilities
Change to IT infrastructure and end user equipment	A process and structure for managing changes to IT-specific infrastructure and end-user devices must be defined. This may be separate from the centralised process and change control committee, as long as it complies with the service delivery policy and process control framework.	The IT&KM division (corporate IT function) is responsible for all IT-specific infrastructure and end-user devices at Rand Water. This function is responsible for defining, implementing and executing the change and configuration management processes and structure for the end-user IT environment.

Table 6-9 Change and Configuration Management - Implementation Illustration

Independent assurance providers provide assurance regarding: 1) the adequacy of the digital service delivery policy; 2) the existence of a process control framework; 3) the change and configuration management processes and procedures; and 4) compliance with the digital service delivery policy and process control framework by the change control committee and the three digital functions of Rand Water. Audit reports are presented to the executive management and the audit committee of the board in this regard.

The following are examples of ***Rand Water characteristics*** that influenced the prioritisation of operational process controls within the context of Rand Water:

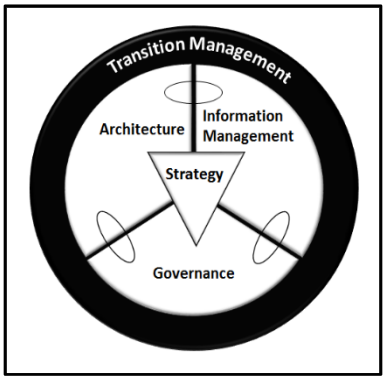
Rand Water Characteristic	Description
Bulk supplier	Rand Water is a bulk supplier of water and sanitation services. It does not collect personal data of citizens via its control systems (e.g. location, water consumption). Privacy and personal information protection therefore only relates to the IT systems managed by one of the three digital functions of Rand Water. This would not be the case if Rand Water was a retail water and sanitation service provider with a demand side management program.
Convergence in digital technology	Rand Water decided to exploit the convergence in digital technology and to integrate the digital infrastructure, in order to achieve the expected benefits (e.g. flow of asset information from control to IT systems). This increased the risk to the overall digital landscape, and has an impact on the prioritisation of operational process controls. Examples of such operational controls are: 1) change and configuration management to reduce the risk of uncontrolled changes; and 2) logical information security to address the ever-increasing cyber security threats to the overall digital landscape via the "weakest link" of the digital environment of Rand Water.

Rand Water Characteristic	Description
Corporate controls and functions	Rand Water has a number of corporate controls that relate directly to the digital process controls, such as a corporate security function and a corporate business continuity plan that applies to all Rand Water functions. Such corporate controls centralise the governance and coordination of an operational process control at a corporate level. Examples of the digital operational controls influenced by the existence of corporate operational controls are: 1) digital business continuity and disaster recovery plans that must integrate and comply with the corporate business continuity plan; and 2) a single unified risk response to the digital risk(s) on the corporate strategic risk register.
Efficiency vs. control	In some cases Rand Water decided to perform some of the non-essential controls in a centralised manner. An example of this is the inclusion of change and configuration management of IT systems into the scope of the single change control committee, which is only required to manage changes to the converged digital infrastructure and digital projects in a centralised manner. This deviation from the prioritisation result is due to practical and efficiency related considerations, rather than risk. The risk based operational process control prioritisation identifies the minimum essential controls, not the maximum, that need to be executed in a centralised manner, in order to adequately mitigate the risk. This deviation to the risk-based prioritisation is therefore allowed.

Table 6-10 Operational Process Controls – Rand Water Context

Rand Water ***received direct benefit*** from the implementation of the digital governance mechanisms, operational process controls and combined assurance model. A number of the security related incidents, that occurred prior to the implementation of the Rand Water Way, seized to occur after the implementation. Examples of such historical incidents are: 1) the failure of the IT and control networks at one of the operational sites, due to uncontrolled after-hours emergency changes made to the network by the control system functions; 2) the failure of the integration of the SCADA data into the IT data warehouse, due to an uncontrolled change made to the SCADA data historian during a SCADA upgrade; and 3) malicious software infecting a SCADA server, and thereafter attempting to infect the IT server hosting the organisation's billing system. Due to the improvement in information security, the organisation is now able to integrate and utilise quality asset information from both the IT and control systems on a continuous basis and in a safe and secure manner for the purpose of evidence-based strategic infrastructure asset management decision making.

6.5. Transition Management



The purpose of this section is to describe the instantiation of the transition management constituent part of the Rand Water Way. It describes the transition roadmap implemented at Rand Water to achieve the future state. It further describes the supporting work streams, namely bedrock factors, project and program management, and organisational change management.

The ***transition roadmap*** of the Rand Water Way was contextualised and applied at Rand Water for defining and completing the journey to reach the desired end state and level of maturity.

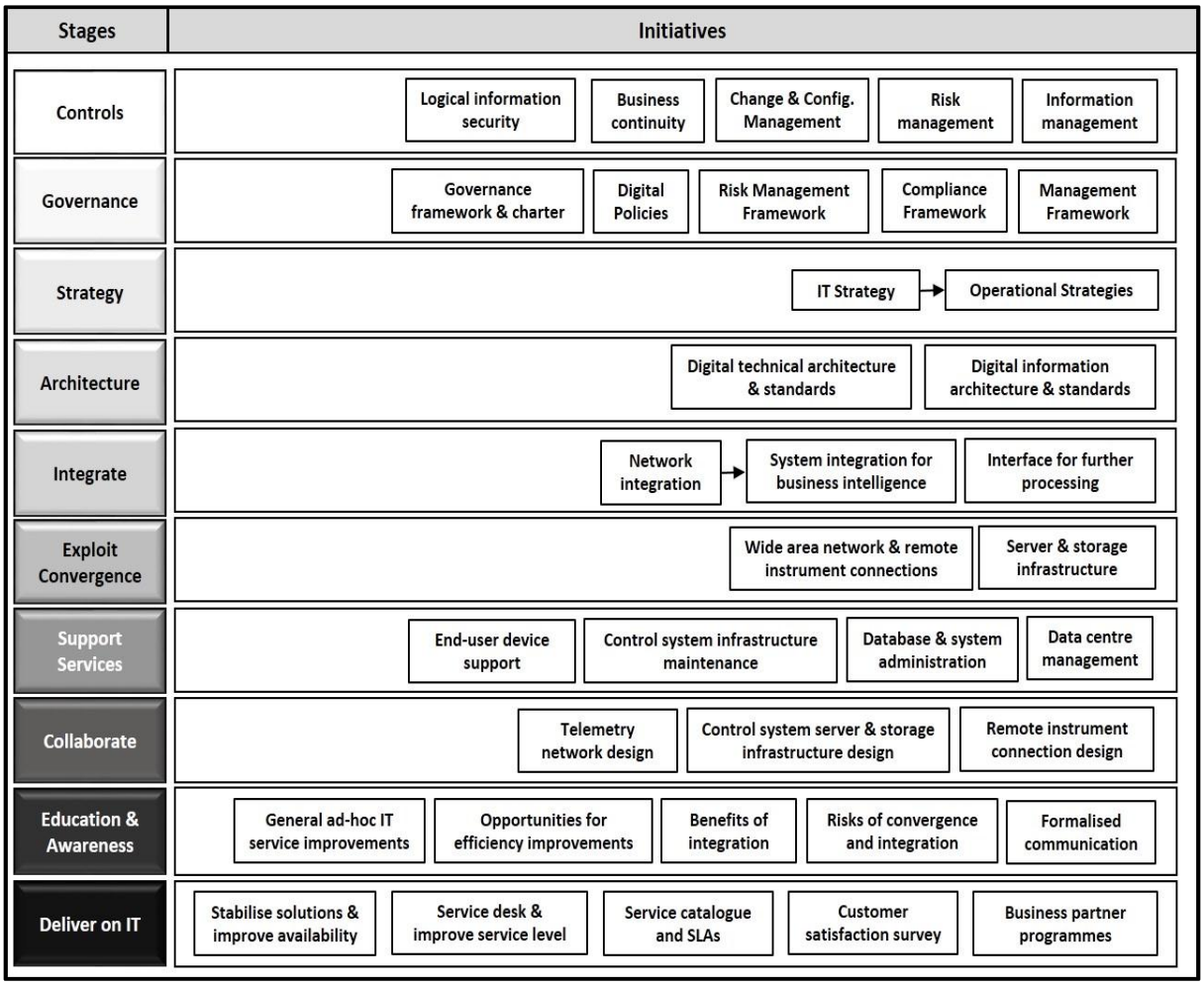


Figure 6-13 Rand Water Transition Roadmap

At the start of this journey in 2007, the Rand Water IT function did not have the credibility or legitimacy to propose or lead this journey. This was primarily due to an ERP system

implementation in 2005 that had significant negative implications for the organisation, as well as an IT network with low availability. There was inadequate trust in the capability of the IT function, as well as in the motive and intention of the function's management. The journey therefore had to start at the lowest level of the roadmap, by focusing on IT service delivery with a "back-to-basics" campaign. There were no short cuts to achieve the desired future state and level of maturity. The application of this roadmap will be illustrated by highlighting the most significant initiatives within each stage along the journey:

Stage	Initiatives
Deliver on IT	The first priority was to stabilise the existing IT solutions and improve the availability of the IT infrastructure. Thereafter, the level of service could be further improved and formalised via an IT helpdesk, involving IT customers in IT decisions, a service catalogue and service level agreement, customer satisfaction surveys, and finally supporting the business units in achieving their business plans via IT solutions.
Education and Awareness	Education and awareness is an ongoing endeavour. The communication subjects changed over time and was synchronised with the specific initiatives of the roadmap. The communication was initially ad-hoc and was aimed at the general user community, digital project governance structures and user groups. It became more formalised over time and included formal communication to the digital steering committee, the executive management and the board of Rand Water.
Collaborate	Collaboration was originally required at Rand Water, due to the scarcity of digital skills. Examples of collaboration projects between IT and control system functions include the design of telemetry networks and remote instrumentation connectivity. Collaboration was also required during the rest of the roadmap. This includes the integration of IT and control digital infrastructure and systems, as well as the design and implementation of digital governance mechanism and operational controls for the control system functions.
Support Service	A number of opportunities were identified, agreed and implemented where the IT function provided shared services to the control system functions. It initially included the low-risk end-user environment infrastructure, such as PCs and printers. It later included control system server and data storage maintenance, database administration and finally the hosting and data center management services for control systems. The emphasis was placed on the work that control system functions were not equipped to do, either in terms of skills or capacity.
Exploit convergence	The convergence in digital technology was exploited, where feasible, and without increasing the risk to the overall digital landscape and the core business of Rand Water to beyond an acceptable level. This included end-user devices (i.e. PCs, printers), servers, data storage and communication networks (i.e. wide area network and links to remote instrumentation).

Stage	Initiatives
Integration	Integration between IT and control systems and the supporting digital infrastructure was driven by business needs. To satisfy these needs the digital infrastructure was first integrated. This was followed up with the integration of control system data into the IT systems landscape for asset management decision making purposes, and thereafter for further processing by IT systems.
Architecture	A Rand Water digital architecture and set of standards were defined, approved and implemented. The technology architecture was first created because it addresses the enabling infrastructure for the digital systems. This was followed by the information architecture and then the security architecture.
Strategy	The overall IT strategy was first defined and approved, in order to provide the overall direction for all digital functions at Rand Water. It was also done to formalise the overall approach and intent, in terms of enterprise-wide digital governance and enterprise-wide asset information management. This was followed up with sub-strategies addressing the details for each of the future states (e.g. how to achieve enterprise-wide digital governance strategy).
Governance	The essential digital governance mechanisms, as determined by the inclusive risk assessment and prioritisation exercise, were designed, approved and implemented. The digital governance framework and charter were implemented first to establish the decision making authority for the remainder of the governance mechanisms. This was followed up with digital policies, a digital risk management framework, a digital compliance checklist and the selection of COBIT as a common foundation for the digital management / process controls.
Control	The essential operational processes controls, as determined by the risk assessment and prioritisation exercise, were designed, approved and implemented. These include change and configuration management of the converged digital infrastructure, digital architecture and standards management, malicious software protection, intrusion protection, information ownership management, and strategic digital risk management. Those threats or weaknesses that posed a higher risk to the organisation were addressed first (e.g. malicious software).

Table 6-11 Rand Water Transition Roadmap Stages

The Rand Water IT function addressed the ***bedrock factors*** before requesting the other digital functions to make any changes to their own environments or practices. The IT function implemented IT system consolidation, IT system integration, operational process controls and IT governance mechanisms prior to requesting any of the two control system functions to do so. The specific IT bedrock factors included: 1) compliance to the King III Code of the Institute of Directors of South Africa and the ICT Governance Framework of the South African Government; 2) an enterprise architecture and set of standards for IT solutions; 3) a business continuity and disaster recovery plan for IT systems; 4) operational IT risk management;

5) an information security management system; 6) a legislative compliance assessment for IT; 7) an enterprise information management framework for data stored in IT systems; as well as 8) change and configuration management for all IT solutions. This assisted with the change management efforts. It ensured that the IT function had the necessary legitimacy to lead this change initiative. It also served as an example of what is expected from the Rand Water control system functions, and thereby increased the predictability and reduced the uncertainty of the desired future state.

A ***program management*** approach was adopted for controlling the work to be performed at Rand Water, as defined by the roadmap. The Rand Water transition roadmap is a medium to long term journey that required a number of discrete projects and some ongoing work, to deliver incremental changes and benefits over time. There were also some opportunistic initiatives, such as the provision of support services and the exploitation of the convergence in digital technology. The scope of every project within the scope of the overall program was therefore not clear at the start of the change journey. This was depended on the pace at which the trust between IT and control system functions improved, as well as the identification of the appropriate opportunities. The overall transition program was overseen by the digital steering committee of Rand Water, which included the appropriate representation from all Rand Water's digital functions and the business units. The project and program management work stream successfully addressed the mechanical side, or "hard-factors", of the change journey and contributed to the success of the overall transition.

Organisational change management was an important aspect of the instantiation of the Rand Water Way. It was explicitly built into the implementation roadmap and the bedrock factor work stream. The focus of the Joint Endeavours and the Cement Foundation phases was to build trust between the IT function and the two control system functions of Rand Water. The trust of the control system functions in the capability and intention of the IT function was improved by: 1) enhancing the IT service and service management maturity; 2) ongoing education and communication efforts; 3) collaboration initiatives between the IT and control system functions; and 4) the IT function providing shared digital support services to the control system functions. These initiatives were executed in a non-threatening manner that: 1) posed no threat to the future existence or organisational structure of the control system functions; and 2) enabled and assisted the control system functions.

The following key interdependent and overlapping organisational change management interventions deployed at Rand Water are highlighted:

Interventions	Description
Build the guiding team	The digital governance framework was co-created by all three digital functions of Rand Water and was approved by the board of Rand Water. The digital governance structures included an appropriate mix of representatives from across Rand Water, including the three digital functions, digital programs and business functions. It allowed the digital steering committee to be utilised as a platform for engagement, knowledge sharing, collaboration and the change management coalition. The head of one of the Rand Water control system functions was appointed as the deputy chair of the Rand Water digital steering committee. The control system functions were involved in all the work performed as part of the roadmap via the digital steering committee, including the prioritisation of process controls. This approach improved buy-in by the control system functions into the transition journey and change management coalition. It also increased the sense of program ownership within the control system functions.
Create vision and strategy	A shared vision was created by and communicated to the digital steering committee. It was followed up with a co-created formalised sub-strategy that defined the desired and shared digital governance future state of Rand Water. The principle regarding enterprise-wide digital governance, rather than organisation centralisation, was agreed upon early on in the change journey. This resolved any uncertainty regarding the future, avoided territorial behaviour, and ensured the future commitment of the control system functions to collaborate with the IT function during the rest of the change journey.
Communicate for buy-in	Two-way communication was a key technique to the overall success of the change, especially during the education and awareness stage of the roadmap. It included communication to business functions, control system functions, executive management and the board of Rand Water. The messages were synchronised with the stages and initiatives of the roadmap, in order to create a sense of urgency and buy-in for the next step to be taken.
Short-term wins	A number of short-term wins were implemented that illustrated the potential benefits before a next step was taken, in order to maintain momentum during the longer term journey. An acceptable level of residual risk related to some of these short-term wins, was accepted. It also provided the control system functions with adequate time to evaluate the benefits realised from the short-term wins, and getting used to the new situation before the next larger change was proposed or initiated. Examples of such short-term wins are: 1) interfacing SCADA information into the IT business intelligence solution without an enterprise-wide digital architecture, enterprise-wide digital configuration management, and enterprise-wide logical information security controls; and 2) providing digital support services to the control system functions without a formally agreed service catalogue or service level agreement.

Table 6-12 Organisational Change Management Interventions and Mechanisms

Apart from the successful achievement of the overall transition, there was additional evidence observed during the transition journey that illustrated the success of the organisational change management related interventions and efforts. The exploitation of the convergence in digital technology (e.g. wide area network), collaboration projects between IT and control system functions, and the "outsourcing" of certain support and maintenance services to the IT function (e.g. SCADA server maintenance), were primarily proposed by the control system functions and not the IT function. This was a significant positive indication of the increase in trust between the Rand Water digital functions, in terms of intention and capability.

Chapter 7 - Evaluation of the Rand Water Way

The purpose of this chapter is to demonstrate the contribution of the Rand Water Way to the field of information management, in support of effective infrastructure asset management. This will be achieved by evaluating the usage, perceived usefulness and perceived usability of the Rand Water Way, as instantiated at Rand Water, as well as its potential perceived usefulness and usability at similar organisations.

7.1. Evaluation Approach

The ***acceptance*** of the Rand Water Way is tested by evaluating its perceived usefulness and usability *(derived from the Technology Acceptance Model of Davis, 1989).* Usefulness, as applied in this research, is defined as the extent to which the Rand Water Way is useful, or beneficial, in supporting effective infrastructure asset management, by addressing the associated real-world problems within a large, complex heterogeneous infrastructure asset intensive organisation, such as Rand Water. There is a close correlation between usefulness and constructs such as valuable, effectiveness, beneficial, importance and relevance *(Davis, 1989).* Usability, as applied in this research, is defined as the extent to which the Rand Water Way is easy to implement and use. There is a close correlation between usability, or ease of use, and constructs such as simplicity, clarity, flexibility, compatibility and convenience *(Davis, 1989).* A third evaluation concept, besides usefulness and usability, is usage *(Keen & Sol, 2008).* The Rand Water Way needs to be operationalised and used in practice, for it to be successful and "measureable" *(Gonzalez & Sol, 2012).* The Rand Water Way is an instantiated artefact at Rand Water. The usage, perceived usefulness and perceived usability of the instantiated Rand Water Way will be evaluated. The potential perceived usefulness and potential perceived usability of the Rand Water Way, will also be evaluated for organisations similar to Rand Water.

Case	Usage	Usefulness	Usability
Rand Water base case	●	●	●
Similar organisations or case studies		● *Potential*	● *Potential*

Table 7-1 Evaluation Criteria per Case Study Category

This will be achieved by determining the potential of contextualising and implementing the generalised Rand Water Way at these organisations to: 1) support and enable effective infrastructure asset management; and 2) effectively address the associated problems at these organisations.

The primary ***instrument*** for the evaluation is expert interviews with a ***panel of experts***. For the evaluation at Rand Water, the expert panel includes representatives from the IT function, the two control system functions and the infrastructure asset management function. The position that fulfils the role of the Chief Information Officer (e.g. CIO, CTO, and CXO) was selected for the evaluation at similar organisations. This role is responsible for enterprise-wide information management at the organisation, including the infrastructure asset management decision support system. The ***organisations participating in this evaluation*** satisfy three criteria, namely: 1) it must be an industrial organisation that is infrastructure asset intensive or infrastructure asset dependent; 2) it must have an IT system landscape and a control system landscape; and 3) it must be a large, complex, and heterogeneous organisation. The size, complexity and heterogeneous nature of the organisation are characterised by its organisational foot print, revenue, number of staff members and value of its infrastructure assets. It is the aim of the evaluation to go beyond the water and sanitation industry, in order to test the generalisability of the Rand Water Way. It therefore includes organisations from the manufacturing, logistics and mining industries. The majority of the organisations are South African organisations. This is due to practical considerations, such as access to the experts. The involvement of the organisations in this evaluation is voluntary. The details regarding the participants are presented in ***Annexure B.***

A ***questionnaire*** is used as an instrument for facilitating the ***expert interviews***, recording the outcome of the interviews, and analysing the information provided. The questionnaire includes both a quantitative and qualitative part. The quantitative part consists of positively stated statements regarding the Rand Water Way's perceived usefulness and usability *(Suaro & Lewis, 2011).* The format of the quantitative ***evaluation statements*** is based on a 5-point Likert scale *(Jamieson, 2004),* namely:

1 = Strongly disagree
2 = Disagree
3 = Neutral
4 = Agree
5 = Strongly agree

The mean, mode and standard deviation are calculated for each statement. This is used to determine the general and most common opinions of the participants, and whether there is general consensus amongst the participants. The usefulness related criteria consist of two sections, namely; section 1 - the degree to which those problems defined in chapter 4 are relevant to the specific organisation; and section 2 - the degree to which the Rand Water Way will resolve, or address, the relevant problems. In the qualitative part, the expert panel members are requested to add their remarks in support of the quantitative feedback. The remarks include the advantages and shortcoming of the Rand Water Way, in relation to the characteristics of the participating organisations.

The ***criteria*** for evaluating the Rand Water Way's ***usefulness*** are as follows:

A - Usefulness Criteria	
1	**Problem Relevance –** *in relation to the specific organisation.*
1.1	**Technology and Information Problems**
1.1.1	**Digital technology size and complexity:** The digital technology landscape, including IT and control systems, is large, complex and heterogeneous.
1.1.2	**Digital isolation and incompatibility:** Control systems are isolated and / or incompatible with IT systems and does not allow asset information to be exchanged between control systems and IT systems.
1.1.3	**Fast pace of digital technology development:** Digital technology and convergence between control and IT system technology are developing at a fast pace.
1.1.4	**Diverse asset information source:** Asset information originates and is stored across the digital landscape (control systems and IT systems).
1.1.5	**Inconsistent asset information management:** Asset information is not managed consistently and rigorously enough across the digital (control and IT systems) landscape (e.g. naming conventions, format, data quality, classification, ownership).
1.1.6	**Big Data:** Asset information volume (e.g. storage size, number of data items, data granularity) and variety (e.g. format, medium) is high and increasing.
1.2	**Process Problems**
1.2.1	**Security threats:** Information or cyber security (i.e. availability, integrity, confidentiality) threats (e.g. malicious software, unauthorised access, natural disasters) pose a risk to the overall digital landscape, especially in the case of an integrated digital landscape.
1.2.2	**Governance maturity inconsistency:** The maturity of digital governance and operational controls differ between control and IT system functions and / or solutions.
1.2.3	**Compliance as end goal:** The primary purpose of digital / IT governance is compliance to a standard, code or framework rather than as a means to reduce the inherent operational digital and information risks.

A - Usefulness Criteria	
1.2.4	**Operational control inadequacy:** The operational process controls of the control systems (e.g. change and configuration management, access control) does not provide adequate assurance that quality data will be made available timeously for asset decision making.
1.2.5	**Lack of alignment:** There is no alignment between the control systems and IT functions in terms of future direction, to-be / vision architecture and common strategic goals.
1.3	**People & Organisational Problems**
1.3.1	**Organisational structure:** The control system and IT functions report into separate / different functional / organisational / business units.
1.3.2	**Lack of trust:** There is a lack of trust in the IT system function by the control system function(s) either in terms of capability (e.g. credibility, capacity, skills, track record) and / or intention (e.g. empire building), leading to a lack in legitimacy to lead this journey.
1.3.3	**Resistance to change:** There is resistance to change by control system functions and / or IT functions, including this change.
1.3.4	**Lack of vision and/or urgency to change:** There is a lack of an agreed shared vision related to digital governance and/or a sense of urgency to change.
1.3.5	**Lack of change forum / coalition:** There is a lack of a change forum or coalition that will market, support and/or drive this change (e.g. team, committees, etc.)
1.3.6	**Lack of collaboration and sharing:** There is a lack of collaboration (e.g. joint projects), resource / skills / expertise sharing (e.g. support services; security threats), involvement in decision making and / or communication between IT and control system functions.
2	**Problem Resolution –** *A contextualised version of the Rand Water Way …*
2.1	**Technology and Information Problem Resolution**
2.1.1	**Complexity, size and pace of change:** Addresses the complexity, size and fast pace of change and convergence of the digital (control system & IT) landscape.
2.1.2	**Asset information exchange:** Assists in enabling asset information to be exchanged between control systems and IT systems for decision support and / or further processing.
2.1.3	**Asset information fusion:** Assists in ensuring that the required asset information from across the digital landscape is fused or harmonised to provide an integrated set of asset information in support of asset decision.
2.1.4	**Asset data quality:** Assists in ensuring that asset information has the required level of quality (e.g. completeness, correctness) to support effective asset decision making.
2.2	**Process Problem Resolution**
2.2.1	**Cyber security threats:** Assists in ensuring that the digital / cyber security (i.e. availability, integrity, confidentiality) threats and risks are adequately mitigated for the integrated digital landscape, including the "weakest links".
2.2.2	**Lack of operational controls:** Adequately addresses the risk related to the lack of operational controls (e.g. change and configuration management), including the related common operational or strategic digital risks.
2.2.3	**Value delivery beyond compliance**: Assists in ensuring that the governance mechanisms and operational process controls deliver value beyond compliance to a regulation, code, standard or framework (e.g. risk mitigation, real pain points).

A - Usefulness Criteria	
2.2.4	**Avoid over and under-regulation:** Prevents the negative implications of over and under regulation of the digital environment, namely inadequate risk reduction and / or inefficiency / productivity loss.
2.3	**People and Organisational Problem Resolution**
2.3.1	**Improve involvement and commitment:** Ensures involvement and / or commitment from all internal stakeholders across the organisation to this change journey and related decision making.
2.3.2	**Reduce resistance to change:** Reduces and / or eliminates the resistance to this change in the way of thinking about digital governance within the organisation.
2.3.3	**Improve trust:** Improves the trust between the digital functions in terms of capability and / or intention and thereby the credibility and legitimacy of the IT function to propose and/or lead this change
2.3.4	**Improve collaboration and sharing**: Improves the collaboration and communication between the digital functions of the organisation, as well as the sharing or skills and expertise.
2.3.5	**Shared vision and direction:** Ensures a common, aligned and shared vision and future direction for the digital functions, especially related to ICT governance.
2.3.6	**Sustainability of change:** Ensures a sustainable change in the way of thinking about digital governance across the organisation. Digital functions will continue to comply with the agreed governance mechanisms and operational controls ("make it stick"; embed the change).

Table 7-2 Usefulness Evaluation Criteria

The ***criteria*** for evaluating the Rand Water Way's ***usability*** are as follows:

B - Usability Criteria	
1	**Simplicity and clarity**
1.1	**Simple:** The philosophy and underlying principles are simple, logical and straightforward.
1.2	**Understandable / clear:** It is clear and easily understandable, including the philosophy, principles, framework and the constituent parts of the approach.
1.3	**Adequately described:** The approach, including its constituent parts, are adequately defined and described.
2	**Compatibility and flexibility**
2.1	**Compatible:** It is compatible with the organisation (e.g. organisational structure; corporate governance structures, culture).
2.2	**Adequate guidance:** Adequate guidance is provided in terms of the contextualisation for and implementation of the Rand Water Way at the organisation.
2.3	**Flexible / adaptive:** It is flexible, generic and adaptable enough to be contextualised for the organisation, where needed.

Table 7-3 Usability Evaluation Criteria

The questionnaire and criteria were pre-tested within Rand Water. The result was used to refine the criteria and statements, in order to improve the usability of the questionnaire (e.g. time to complete the interview) and the consistent interpretation of the statements by the expert panel

members. In addition, refinements were made to the questionnaires used for the evaluation of the instantiated artefact at Rand Water versus the evaluation of the potential usefulness and usability of the Rand Water Way at similar organisations. This includes: 1) stating the statements in past tense for the evaluation of the instantiated artefact at Rand Water; 2) using terminology that the Rand Water digital functions are familiar with; and 3) requesting additional organisational details for the evaluation at other similar organisations. The questionnaires used for the evaluation are presented in ***Annexure B.***

7.2. Evaluation of Rand Water Instantiation

The Rand Water Way is firstly evaluated in terms of ***usage.*** The Rand Water Way was contextualised, approved and implemented at Rand Water, as demonstrated in chapter 6. The Rand Water IT Strategy was formalised and approved by the organisation's executive management committee and the board of directors. This includes the principle that directs enterprise-wide digital governance in support of infrastructure asset management. The strategy formalises the buy-in from Rand Water's executive management and board of directors. It also directs the rest of the constituent parts of the Rand Water Way (i.e. Architecture, Information Management, Governance, and Transition Management) and the three digital functions within Rand Water. The enterprise-wide digital architecture and standards were formalised and approved by the digital steering committee. It was implemented and is being complied with by all Rand Water's digital functions and projects. Asset information from across the digital landscape is being managed as an enterprise resource to ensure the timely availability of quality data for asset decision making. The digital governance framework and policies were formalised and approved by the organisation's executive management committee and board of directors, and was implemented. The selected operational digital controls were agreed upon by all digital functions, via a risk assessment, and were implemented. All digital functions comply with the selected digital governance mechanisms (e.g. governance framework, policies) and operational process controls. The transition management roadmap was defined, accepted by the digital steering committee, and applied. The transition, or change, was successfully achieved across all three digital functions of Rand Water. The Rand Water Way is operational and used at the base case, Rand Water.

The Rand Water Way is secondly evaluated in terms of its ***perceived usefulness***. The expert panel was requested to respond to the problem relevance section based on the situation at the start of the Rand Water transition journey, namely 2007.

The result of the evaluation of the perceived usefulness of the Rand Water Way at Rand Water is as follows:

	Usefulness Criteria	Mean	Standard Deviation	Mode
A	**Usefulness**	**4.25**	**0.46**	**4.00**
A.1	**Problem relevance**	**3.92**	**0.94**	**4.00**
A.1.1	**Technology and information problems**	**3.93**	**0.87**	**4.00**
1.1.1	Digital technology size and complexity	4.29	0.76	4.00
1.1.2	Digital isolation and incompatibility	3.14	1.07	4.00
1.1.3	Fast pace of digital technology development	3.57	1.13	4.00
1.1.4	Diverse asset information sources	4.29	0.49	4.00
1.1.5	Inconsistent asset information management	4.00	0.58	4.00
1.1.6	Big data (volume, variety)	4.29	0.49	4.00
A.1.2	**Process problems**	**4.03**	**0.89**	**4.00**
1.2.1	Security threats	4.43	0.53	4.00
1.2.2	Governance maturity inconsistency	4.57	0.53	5.00
1.2.3	Compliance as end goal	3.43	1.40	2.00
1.2.4	Operational control inadequacy	3.57	0.79	4.00
1.2.5	Lack of alignment	4.14	0.38	4.00
A.1.3	**People and organisational problems**	**3.81**	**1.04**	**4.00**
1.3.1	Organisational structure	4.71	0.49	5.00
1.3.2	Lack of trust	3.29	1.11	4.00
1.3.3	Resistance to change	3.43	0.98	4.00
1.3.4	Lack of vision and/or urgency to change	3.57	1.13	4.00
1.3.5	Change forum / coalition	4.00	1.15	5.00
1.3.6	Lack of collaboration and sharing	3.86	0.90	4.00
A.2	**Problem resolution**	**4.15**	**0.57**	**4.00**
A.2.1	**Technology and information problem resolution**	**4.09**	**0.59**	**4.00**
2.1.1	Complexity, size and pace of change	4.13	0.64	4.00
2.1.2	Asset information exchange	4.25	0.46	4.00
2.1.3	Asset information fusion	4.00	0.76	4.00
2.1.4	Asset data quality	4.00	0.53	4.00
A.2.2	**Process problem resolution**	**4.10**	**0.62**	**4.00**
2.2.1	Cyber security threats	4.38	0.52	4.00
2.2.2	Lack of operational controls	4.00	0.53	4.00
2.2.3	Value delivery beyond compliance	4.00	0.63	4.00
2.2.4	Avoid over and under-regulation	4.00	0.82	4.00
A.2.3	**People and organisational problem resolution**	**4.21**	**0.54**	**4.00**
2.3.1	Improve involvement and commitment	4.25	0.46	4.00
2.3.2	Reduce resistance to change	4.00	0.53	4.00
2.3.3	Improve trust (between digital functions)	4.25	0.46	4.00
2.3.4	Improve collaboration and sharing	4.25	0.71	4.00
2.3.5	Shared vision and direction	4.38	0.52	4.00
2.3.6	Sustainability of change	4.13	0.64	4.00

Table 7-4 Usefulness Evaluation Result at Rand Water

Generalised statements were constructed using the most common phrases used by the Rand Water expert panel members in the remarks section of the questionnaire and during the interviews.

The most significant statements regarding the usefulness of the Rand Water Way are as follows:

Generalised Usefulness Remarks
Advantages and strengths
The Rand Water digital landscape is large, complex and heterogeneous.
The integration, exchange and harmonisation of diverse asset information sources from across the IT and control system landscape is a key advantage of the approach.
The split between the two disciplines, namely IT and control systems, is becoming grey due to the convergence in digital technology.
All the digital solutions are incorporated into Rand Water's enterprise architecture, including the technical and information architectures.
A common asset information management approach (e.g. data ownership, data quality, formats) is necessary and important.
The approach strikes a good balance between compliance, optimal operations and risk mitigation.
The governance mechanisms and operational process controls implemented for the digital landscape, including control systems, are beneficial.
The major problems addressed by the approach are digital governance and information security, especially due to the integration of the IT and control systems landscape.
IT is ahead of the control system functions in terms of digital governance. The digital governance practices successfully applied by the IT function, can be considered as best practice and be extended to the control systems environment.
The formalised commitment and buy-in of the executive team obtained via this approach is an advantage (e.g. approved strategy, digital governance framework, and digital policies).
The three digital functions need to work together and alignment between IT and control system functions is of vital importance going forward. Co-operation between the digital functions is formalised by this approach.
All digital functions were involved in the design, approval and implementation of the approach.
The change is sustainable within the Rand Water digital environment.
Disadvantages and shortcomings
Integration of the IT and control system landscapes significantly increased the risk to the infrastructure installation, due to potential malicious software attacks.
Even with the balanced governance stance, this approach might still be seen at an operational level of the control system functions as additional "red tape" driven by IT.
The role of the digital steering committee is not always known, or agreed upon, across the organisation and other governance structures (e.g. supply chain structures).
Performance management, as an instrument to improve co-operation and reduce resistance to change, is not utilised by the approach.
There is a difference between the skills sets, capacity, mind set and culture of the IT function versus control systems functions (e.g. urgency to repair a fault, need for 24x7 availability). The changes might not be adequately addressed and might remain a concern.
Lack of clarity regarding the overall accountability for the successful implementation and sustainable maintenance and support of the resulting governance mechanisms and operational controls is a concern.

Table 7-5 Generalised Rand Water Usefulness Remarks

The results of the quantitative evaluation of the ***usability*** of the Rand Water Way at Rand Water is as follows:

	Usability Criteria	Mean	Standard Deviation	Mode
B	**Usability**	**3.75**	**0.71**	**4.00**
B.1	**Simplicity and clarity**	**3.50**	**0.93**	**4.00**
B.1.1	Simple	3.50	0.93	3.00
B.1.2	Understandable / clear	3.38	1.06	4.00
B.1.3	Adequately described	3.63	0.92	4.00
B.2	**Compatibility and flexibility**	**4.00**	**0.85**	**4.00**
B.2.1	Compatible	4.13	0.64	4.00
B.2.2	Adequate guidance provided	3.50	1.07	4.00
B.2.3	Flexible / adaptive	4.43	0.53	4.00

Table 7-6 Usability Evaluation Result at Rand Water

The most significant statements of the Rand Water expert panel regarding the usability of the Rand Water Way are as follows:

Generalised Usability Remarks
Advantages and strengths
The approach is a well-crafted theory and strategy, but is still a bit theoretical.
The overall philosophy and principles are easy to understand and straightforward.
The approach is compatible with Rand Water's organisation structure, culture and corporate governance.
Disadvantages and shortcomings
The implementation of the related topics (e.g. enterprise architecture, information management, governance) is not simple or easy.
The difficulty is in the implementation, or operationalisation, of the approach at a practical level.
A lot of effort is required to fully implement the approach, especially by the control system functions (e.g. refining and implementing digital policies and operational controls).
It is flexible enough to be adapted by the organisation and to cater for changes in the organisation (e.g. mergers and acquisitions).

Table 7-7 Generalised Rand Water Usability Remarks

There is agreement amongst the expert panel members that the Rand Water ***digital technology and information*** landscape is large, complex and heterogeneous. There is also agreement regarding the need to harmonise the diverse asset information from IT and control systems in support of infrastructure asset management decisions, via an enterprise-wide digital architecture and common enterprise-wide information management practices. However, there is a difference of opinion *(standard deviation above 1.00)* regarding the incompatibility and fast pace of change of digital technology. The majority of control system representatives are of the opinion that control systems are not developing at a fast pace at Rand Water and that control

systems are compatible with the IT systems. The primary underlying reasons for this difference of opinion are the convergence in digital technology and the existence of common industry standards and network protocols that reduce the risk of incompatibility and enable the integration of IT and control systems. Another reason is that the automation (SCADA) environment at Rand Water is fairly stable at this point, and that Rand Water has been fairly conservative to date in terms of adopting new technology that impacts the essential core business processes. The IT and Scientific Services environments, on the other hand, are experiencing a faster pace of change. There is general consensus amongst the expert panel members that the Rand Water Way approach effectively addresses the technology and information related problems.

There is agreement amongst the expert panel members that the ***process*** related problems (e.g. security, governance) are relevant to the Rand Water environment and that the Rand Water Way effectively addresses these problems. There is a difference of opinion between the IT function and control system function participants regarding compliance being considered as an end in itself, rather than a way to deliver value by reducing operational risk. This difference of opinion exists because the board of Rand Water decided that the IT function must comply with the King III Code and the South African Government IT governance framework. However, such compliance is not applicable to the control system functions. There is agreement that there is a difference between the maturity of digital governance at the three digital functions, especially between the Automation function (i.e. SCADA) and the other two digital functions. There is general consensus amongst the participants that the Rand Water Way strikes a good balance ("optimal operational risk mitigation") between over and under regulation of the Rand Water digital environment. The participants also agree that the digital governance mechanisms and operational process controls selected and implemented at Rand Water, are beneficial ("deliver value") to the organisation.

There is a difference of opinion between the participants regarding the existence of the majority of ***people and organisational*** related problems within the Rand Water digital environment, such as: 1) resistance to change by digital functions; 2) lack of a change forum / coalition; 3) a lack of shared vision; and 4) a lack of urgency to change. There is agreement amongst the expert panel members regarding: 1) the lack of involvement and sharing between the digital functions; and 2) the separation of the digital functions of Rand Water. The difference of opinion is evident between the IT function representatives and the control system and asset management representatives. The IT function representatives agree, to strongly agree, that the

people related problems exist, especially within the control system functions. The participants from the control system functions do not agree with this opinion. There is consensus amongst the participants that there is a need for the Rand Water digital functions to work together and that the Rand Water Way facilitates collaboration, by: 1) involving control system function in the design, approval and implementation of the Rand Water Way; and 2) obtaining formal commitment and buy-in from executive management and the board of the organisation for the approach. The participants have some concerns regarding people related problems that might not be adequately addressed by the Rand Water Way, such as: 1) the continued involvement, commitment and view of "grass roots" staff members; and 2) unclear accountability for the success of the Rand Water Way.

There is a difference of opinion regarding some of the ***usability*** criteria, namely: 1) the simplicity and clarity of the approach; and 2) adequacy of implementation guidance provided. The Automation (SCADA) and Infrastructure Asset Management participants disagree with these usability statements, whilst the IT and Scientific Services Information Management participants agree with these statements. There is agreement between the participants that the overall philosophy and principles are understandable and straight forward, but that the constituent parts of the approach (e.g. architecture, information management, governance) and the implementation of the approach is not simple or easy. It requires extensive guidance, facilitation, management commitment, and dedicated staff, in order for the philosophy and principles to be successfully operationalised across the digital functions. There is also agreement that the Rand Water Way is compatible with the Rand Water organisational structure, culture and corporate governance structures. There is further agreement that the Rand Water Way is flexible and adaptable enough to be tailored and contextualised for the organisation, as well as to cater for future changes to the organisation.

Notwithstanding the concerns raised and some difference of opinion, there is a ***general acceptance*** of the Rand Water Way by the Rand Water expert panel members, in terms of its perceived usefulness and usability. The mean response from the expert panel to the usefulness statements is positive (4.25 = between agree and strongly agree), the standard deviation is less than 1.00 (0.46) and the mode is 4 (agree). The mean response from the expert panel to the usability statements is positive (3.75 = between neutral and agree), the standard deviation is less than 1.00 (0.71) and the mode is 4 (agree). All (100%) of the rounded off mean responses per expert panel member to the usefulness related statements are positive (i.e. agree or strongly agree). The rounded off mean response of approximately two thirds (63%) of the panel

members to the usability related statements are positive (i.e. agree or strongly agree) and approximately one third (38%) are neutral. None of the mean responses per expert panel member to the usefulness or usability related statements are negative (i.e. disagree or strongly disagree).

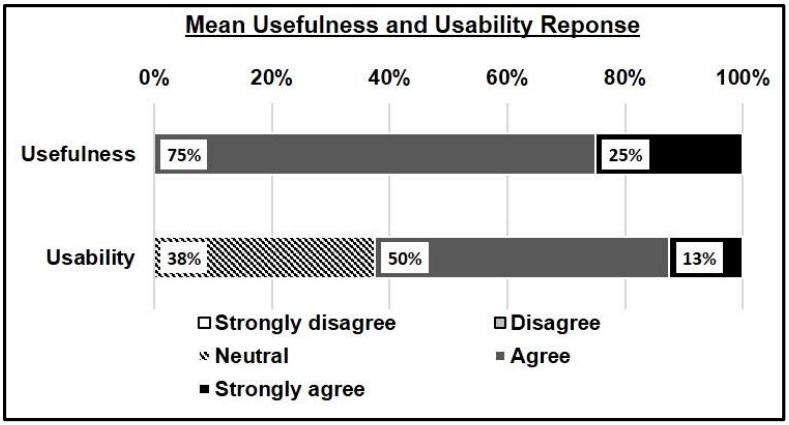


Figure 7-1 Rounded-Off Mean Response of Rand Water Panel

The Rand Water Way is perceived to be useful and usable in addressing the related problems at Rand Water, in support of infrastructure asset management. It is overall considered as: 1) necessary for Rand Water; 2) the correct direction for Rand Water; 3) a well balanced approach, 4) applicable to Rand Water, and 5) beneficial to Rand Water. The detailed Rand Water usefulness and usability evaluation related responses are presented in ***Annexure B.***

7.3. Evaluation at Similar Organisations

The ***organisations that participated*** in this evaluation are as follows:

Organisation	Description
Org # 1	A South African subsidiary of a London-based multi-national brewery.
Org # 2	An African state-owned national postal service provider.
Org # 3	A multi-national South African based iron ore mining company in the private sector.
Org # 4	A South African subsidiary of a multi-national consumer goods (FMCG) manufacturer in the private sector.
Org # 5	A South African-based multinational platinum mining company in the private sector.
Org # 6	A South African cement manufacturer in the private sector with an African continental foot print.
Org # 7	A South African subsidiary of a global soft drinks manufacturer in the private sector.
Org # 8	A South African state owned retail water and sanitation utility with a metropolitan / municipal foot print.
Org # 9	A South African state owned water and sanitation utility with a regional foot print.

Table 7-8 Participating Organisations

Two thirds of the participating organisations are from the private sector. The remaining third are state owned entities (i.e. public sector), like Rand Water. The evaluation will therefore test the potential usefulness and usability of the Rand Water Way for both private and public sector organisations.

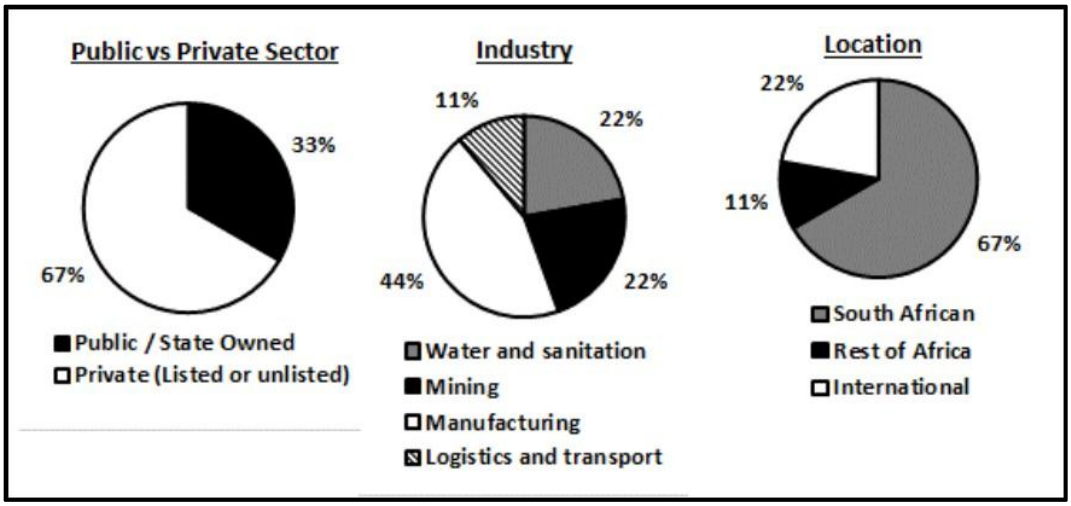


Figure 7-2 Sector, Industry and Location Analysis

Two thirds of the participating organisations are South African organisations. One participant is from the rest of Africa and two participants are global or multi-national organisations. The South African organisations include South African-based multi-national organisations. The evaluation will therefore test the potential usefulness and usability of the Rand Water Way for South African, African and international organisations. The participating organisations are from the water and sanitation, mining, logistics and transport, and manufacturing industries. The manufacturing industry represents 44% of the participants. It includes a variety of products, such as multi-brand fast moving consumer goods, cement, beer and soft drinks. There are two participants from the same industry as Rand Water, namely the water and sanitation industry. The evaluation will therefore test the generalisability of the Rand Water Way, by evaluating its potential usefulness and usability for asset intensive organisations beyond the water and sanitation industry.

Nearly one quarter of the participating organisations are of a similar size than Rand Water and nearly half of the participating organisations are larger than Rand Water in terms of their infrastructure asset value and revenue. Approximately three quarters of the participating organisations are larger and more complex than Rand Water in terms of their organisational foot print. Nearly one third of the participating organisations have more staff than Rand Water and nearly half have a similar staff complement to that of Rand Water. The evaluation will

therefore test whether the Rand Water Way is potentially useful and usable for organisations similar to, smaller, and larger than Rand Water.

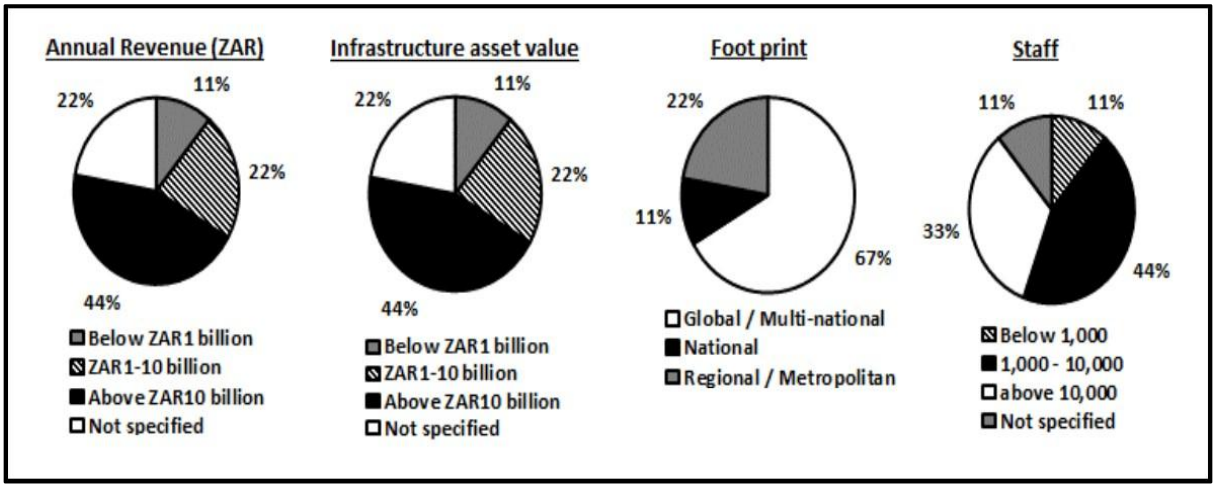


Figure 7-3 Size and Complexity Analysis

Approximately 90% of participating organisations have similar digital organisations to that of Rand Water (i.e. a corporate IT function reporting to a CIO and control system functions reporting to the core business). Only one of the participating organisations has a single digital function that is responsible for both IT and control systems. The evaluation will therefore primarily test the potential usefulness and usability of the Rand Water Way for organisations with a segregated IT and control system organisation. The digital landscapes of the participating organisations are very similar to the Rand Water digital landscape (i.e. ERP, SCADA, LIMS), even though the specific software products differ. The Chief Information Officer, or equivalent role within the participating organisation, was the primary participant in the evaluation. Where possible, the head of the control system function was also involved (e.g. Chief Technology Officer). A summary of the Rand Water Way, including content from chapters 1 to 6 of this dissertation, was provided to each of the participants in preparation for the evaluation.

The result of the evaluation of the potential ***usefulness*** of the Rand Water Way for organisations similar to Rand Water is as follows:

	Usefulness Criteria	Mean	Standard Deviation	Mode
A	**Usefulness**	**3.83**	**0.35**	**4.00**
A.1	**Problem relevance**	**3.67**	**1.15**	**4.00**
A.1.1	**Technology and information problems**	**4.02**	**0.96**	**4.00**
1.1.1	Digital technology size and complexity	4.33	0.71	5.00
1.1.2	Digital isolation and incompatibility	3.33	1.12	4.00

	Usefulness Criteria	Mean	Standard Deviation	Mode
1.1.3	Fast pace of digital technology development	4.00	0.87	4.00
1.1.4	Diverse asset information sources	4.56	0.53	5.00
1.1.5	Inconsistent asset information management	3.56	1.24	4.00
1.1.6	Big data (volume, variety)	4.33	0.71	5.00
A.1.2	**Process problems**	**3.56**	**1.25**	**4.00**
1.2.1	Security threats	4.67	0.50	5.00
1.2.2	Governance maturity inconsistency	3.89	0.93	4.00
1.2.3	Compliance as end goal	3.22	1.30	2.00
1.2.4	Operational control inadequacy	3.00	1.32	4.00
1.2.5	Lack of alignment	3.00	1.32	4.00
A.1.3	**People and organisational problems**	**3.43**	**1.18**	**4.00**
1.3.1	Organisational structure	4.78	0.44	5.00
1.3.2	Lack of trust	2.89	1.17	4.00
1.3.3	Resistance to change	3.22	0.97	4.00
1.3.4	Lack of vision and/or urgency to change	3.11	1.27	4.00
1.3.5	Change forum / coalition	3.22	1.09	4.00
1.3.6	Lack of collaboration and sharing	3.33	1.12	4.00
A.2	**Problem resolution**	**3.90**	**0.73**	**4.00**
A.2.1	**Technology and information problem resolution**	**3.97**	**0.74**	**4.00**
2.1.1	Complexity, size and pace of change	3.67	0.87	4.00
2.1.2	Asset information exchange	4.11	0.78	4.00
2.1.3	Asset information fusion	4.00	0.50	4.00
2.1.4	Asset data quality	4.11	0.78	4.00
A.2.2	**Process problem resolution**	**4.00**	**0.68**	**4.00**
2.2.1	Cyber security threats	4.22	0.83	5.00
2.2.2	Lack of operational controls	4.11	0.78	4.00
2.2.3	Value delivery beyond compliance	3.78	0.44	4.00
2.2.4	Avoid over and under-regulation	3.89	0.60	4.00
A.2.3	**People and organisational problem resolution**	**3.80**	**0.76**	**4.00**
2.3.1	Improve involvement and commitment	3.56	0.88	4.00
2.3.2	Reduce resistance to change	3.33	0.87	3.00
2.3.3	Improve trust	3.89	0.60	4.00
2.3.4	Improve collaboration and sharing	4.00	0.71	4.00
2.3.5	Shared vision and direction	4.00	0.71	4.00
2.3.6	Sustainability of change	4.00	0.71	4.00

Table 7-9 Usefulness Evaluation Result at Similar Organisations

Generalised statements were constructed using the most common phrases in the remarks made by the expert panel members. The most significant statements regarding the usefulness of the Rand Water Way are as follows:

Generalised Usefulness Remarks
Advantages and strengths
It is a well-balanced and pragmatic approach that ensures compliance, whilst allowing adequate operational freedom in terms of operational decisions by digital functions. This is achieved by addressing and separating the governance and operational / management layers of control.

Generalised Usefulness Remarks
It improves governance within the control system function, by implementing the same rigor of an IT function for the control systems.
It aims at sustainable longer term value. It is not a rushed implementation, but also delivers short-term benefits.
It fosters collaboration, cooperation, sharing and alignment between IT and control system functions. It provides a good basis to sell or market the change and to obtain buy-in.
It is applicable to large and complex digital environments, including all organisations that have IT and control systems, and that require integration between IT and control systems.
Disadvantages and shortcomings
The transition and change management approach should be supplemented with measures to enforce the new way of working, such as the performance management system of the organisation.
IT is seen as driving the transition, instead of an executive of the organisation. This puts a lot of pressure on IT to ensure a successful change that requires other digital functions to cooperate. A lot of influencing is required for the change to be successful.
Digital architecture, standards, systems (products) and vendors differ significantly between infrastructure installations and countries, for a multi-national organisation.

Table 7-10 Generalised Usefulness Remarks by Similar Organisations

There is agreement (agree to strongly agree) amongst the participants that the problems related to the size and complexity of the asset ***information*** ("big data") and the underlying ***digital technology,*** as well as the pace of digital technology change are relevant to their organisations. There was a difference of opinion (a standard deviation of more than 1.00) about problems in their organisations regarding digital technology isolation and incompatibility, as well as inconsistent asset information management practices between IT and control system functions. There is agreement amongst the participants that the Rand Water Way can potentially be useful in their organisations, in that it will address all the technology and information related problems, including data quality and asset information fusion. The participants are also of the opinion that the Rand Water Way is applicable to large and complex asset intensive organisations that require integration between their IT and control systems.

There is a lack of consensus amongst the participants regarding the relevance of the ***process*** related problems to their organisations. There is agreement amongst the participants that problems related to information security threats and inconsistent maturity of governance practices between IT and control system functions, are relevant to their organisations. The majority of participants disagree that compliance is an end goal in itself for digital governance at their organisations. They also disagree that there is a lack of strategic alignment

between the IT and control system functions in their organisations. These organisations already have a shared and aligned future direction for their digital environment, including IT and control system functions. They also focus on delivering value via digital governance, rather than mere complying with any standard, code or framework. The practices and opinions of such companies are in line with the principles proposed by the Rand Water Way. There is a difference of opinion amongst participants about the inadequacy of operational, or management, controls within their organisations. Approximately 50% of participants agree / strongly agree that operational controls in their control system functions are inadequate, whilst the other 50% disagree / strongly disagree. There is agreement amongst the participants that the Rand Water Way can potentially be useful in their organisations, in that it will address all the process related problems, including digital security, governance and operational controls. The participants are also of the opinion that the Rand Water Way is a well-balanced and practical approach in terms of digital governance, and that it avoids the negative consequences of over and under regulation of the digital environment.

There is a significant difference of opinion between participants about the majority of the ***people and organisational*** related problems. The opinions range from strongly agree to strongly disagree. Approximately 50% of these organisations already achieved a degree of collaboration, cooperation, knowledge sharing, and trust between the IT and control system functions. These organisations already addressed the primary elements of stages 1 (Cement Foundation) and 2 (Joint Endeavours) of the Rand Water Way. They have a sound basis and change coalition for progressing with the rest of the roadmap, emphasising efficiency gains and formalisation. The one problem that all participants agree or strongly agree with, is the problem related to the digital organisation structure of the organisation (i.e. segregation of digital functions). There is agreement amongst the participants that the Rand Water Way can potentially be useful in their organisations, in that it will address the majority of the people and organisational related problems. This includes collaboration and sharing between segregated digital functions, as well as a shared direction for all digital functions. A concern was raised by some of the participants that the Rand Water Way by itself might not ensure commitment, involvement, and a sustained change in the way of thinking and working. These participants are of the opinion that other organisational mechanisms, such as performance management, should be used to enforce the change. A concern was also raised that the IT function is seen as driving this change, rather than an executive of the organisation.

The result of the evaluation of the potential ***usability*** of the Rand Water Way in organisations similar to Rand Water is as follows:

	Criteria	Mean	Standard Deviation	Mode
B	**Usability**	**4.00**	**0.71**	**4.00**
B.1	**Simplicity and clarity**	**4.00**	**0.87**	**4.00**
B.1.1	Simple	3.89	0.93	4.00
B.1.2	Understandable / clear	4.00	0.87	4.00
B.1.3	Adequately described	3.67	0.87	4.00
B.2	**Compatibility and flexibility**	**3.78**	**0.67**	**4.00**
B.2.1	Compatible	3.44	0.88	3.00
B.2.2	Adequate guidance	3.67	0.87	4.00
B.2.3	Flexible / adaptive	3.67	0.87	4.00

Table 7-11 Usability Evaluation Result at Similar Organisations

The most significant generalised statements, regarding the usability of the Rand Water Way, are as follows:

Generalised Usability Remarks
Advantages and strengths
The approach is adaptable, flexible and scalable. It is applicable to, and can be replicated in, other asset intensive organisations in other industries.
The approach is well thought through, is clear and is logical.
Disadvantages and shortcomings
Extensive tailoring will be required for the digital governance structure to be applicable to, and appropriate for, multi-national organisations consisting of numerous autonomous business units, or entities. Further development is required in this regard.

Table 7-12 Generalised Usability Remarks by Similar Organisations

The overall assessment of the usability of the Rand Water Way by the participants is positive *(i.e. a mean of 4 and a mode of 4).* Two thirds of the participants agree / strongly agree that the Rand Water Way is usable for their organisations. This includes the simplicity and clarity, as well as the compatibility and flexibility of the approach. There is also agreement between participants *(i.e. standard deviation less than 1),* in terms of the usability of the approach. One concern was raised, namely that extensive tailoring is required for the Rand Water Way to be applicable and compatible to multi-national organisations. This opinion was common amongst the majority of the multi-national organisations that participated in the evaluation.

There is a difference between the responses received from the participants from the different ***industries*** as well as from the ***public versus private sector***. The mean response per industry is as follows:

Industry	Usefulness	Usability	Overall
Water	4.00	4.50	**4.25**
Mining	3.75	3.50	**3.63**
Logistics	4.00	4.00	**4.00**
Manufacturing	3.63	4.00	**3.81**

Table 7-13 Industry Analysis

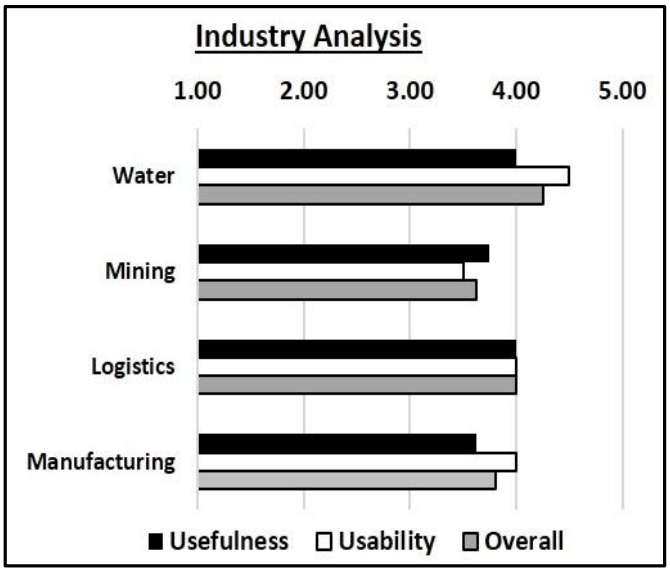


Figure 7-4 Mean Response per Industry

The mean response for the private versus the public (state owned organisations) sector participants is as follows:

Public / Private	Usefulness	Usability	Overall
Public (State)	4.33	4.33	4.33
Private	3.67	3.83	3.75

Table 7-14 Public vs. Private Analysis

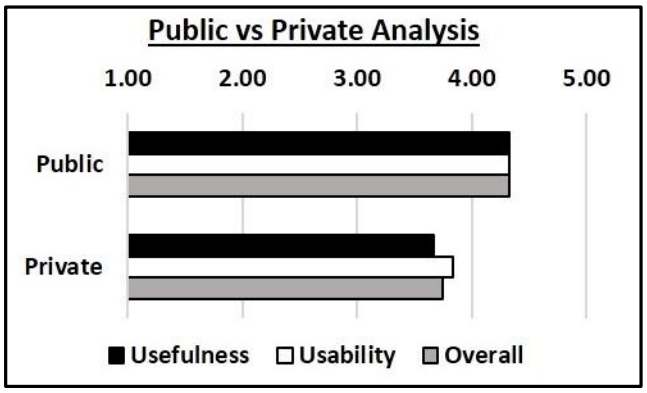


Figure 7-5 Mean Response - Public vs. Private

The water and sanitation industry, which is the same industry as Rand Water, has the most positive response *(i.e. between agree and strongly agree).* The mining and manufacturing industries have the least positive response (i.e. between neutral and agree). The public sector participants, who are in the same sector as Rand Water, have a more positive response than the private sector participants. The first reason for this is that all the multinational, or global, organisations, on the expert panel are private sector organisations from the manufacturing and mining industries. These organisations are of the opinion that the Rand Water Way requires

extensive tailoring in order for the digital governance structure to be useful and usable for multi-national organisations consisting of numerous autonomous business units, or legal entities. The second reason is that the majority of the private sector participants from the manufacturing and mining industries already established trust, collaboration, knowledge sharing and strategic alignment between the digital functions of the respective organisations. There are no other recognisable, or significant, differences between the feedback received from the private versus public sector organisations, or from organisations in different industries.

Notwithstanding the concerns raised and the difference of opinions between some of the expert panel members, there is a general ***acceptance*** of the Rand Water Way, in terms of its perceived potential usefulness and usability. The mean response from the expert panel to the usefulness statements is positive *(3.83 = between neutral and agree),* the standard deviation is less than 1.00 *(0.35)* and the mode is 4 *(agree).* The mean response from the expert panel to the usability statements is positive *(4.00 = agree),* the standard deviation is less than 1.00 *(0.71)* and the mode is 4 *(agree).* All *(100%)* of the rounded off mean response per expert panel member to the usefulness related statements are positive (i.e. agree or strongly agree). The rounded off mean response of three quarters *(75%)* of respondents to the usability related statements are positive *(i.e. agree or strongly agree)* and approximately 20% are neutral. None of the mean responses to the usefulness or usability related statements are negative *(i.e. disagree or strongly disagree).*

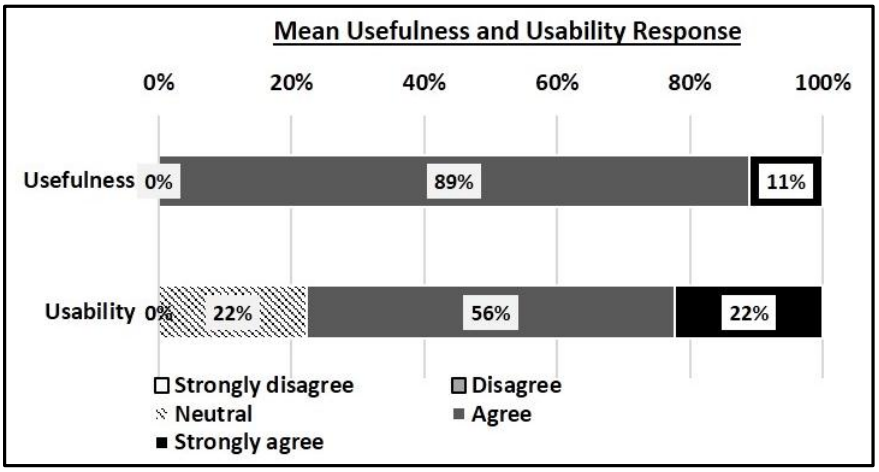


Figure 7-6 Rounded-off Mean Response of Similar Organisations Panel

If a contextualised version of the Rand Water Way is implemented at these organisations, it will address the associated real-world problems within that large, complex heterogeneous infrastructure asset intensive organisation. It is overall considered as: 1) applicable to the organisations; 2) a well-balanced and practical approach; and 3) potentially beneficial to the

organisations. The Rand Water Way is ***perceived to be potentially useful and usable*** in support of infrastructure asset management, at asset intensive organisations across different industries and sectors. The concerns raised will be considered for further research initiatives. The detailed potential usefulness and usability evaluation related responses and the analysis of the most common remarks made by the expert panel members from the participating organisations, are presented in ***Annexure B.***

Chapter 8 - Epilogue

The purpose of this chapter is to present the closing remarks and a reflection on the research. This includes reflecting on the problem relevance, the research rigour, the evaluation of the artefact, the increase in knowledge, and the contribution made by the research. It further provides direction regarding further related research opportunities.

8.1. Problem Relevance

> *The design must address a relevant and important problem and the presentation of the results needs to address the requirements of the professionals* (Hevner, March, Park & Ram, 2004). *Design science research should create and apply an innovative artefact to solve real-world problems* (March & Smith, 1995; Hevner & Chatterjee, 2010).

This research ***originated from a business need*** of the base case, Rand Water, to make evidence-based strategic infrastructure asset management decisions. Rand Water required relevant harmonised quality asset information from both the IT and control systems. The solution involves the integration of heterogeneous multi-source information to provide relevant, consistent, aggregated and meaningful evidence, required to make decisions (Chapters 2). Rand Water is a South African regional bulk water utility delivering a critical national service. It is the largest water utility in Africa (Chapter 3).

A number of ***real-world problems*** were identified that could prevent the successful enablement and support of strategic infrastructure asset management decision making in a sustainable manner at Rand Water (Chapter 4). These problems relate to: 1) the collection and transformation of asset information from different sources into useful and reliable evidence to effectively support strategic infrastructure asset management decision making; and 2) the implementation of a sustainable change regarding asset information management and digital governance across all the digital functions of the organisation (Chapter 4). A new way of thinking, working, controlling and modelling was required in relation to asset information management and digital governance, in order to resolve these problems. An appropriate approach was also required to implement the new way of thinking, working, controlling and modelling in a sustainable manner for a large, complex heterogeneous organisation, such as Rand Water.

The following ***research questions*** were posed (Chapter 1):

1. ***What is the content of a digital governance approach that addresses the information requirements of a modern infrastructure asset management philosophy and the associated problems?***

   The objective of this research question is to determine the appropriate digital governance approach that would add value to the organisation, by enabling enterprise-wide asset information management in support of infrastructure asset management. It should mitigate the related risks, without having a negative influence on the need of the control system function(s) to support the core business efficiently and effectively on a 24x7 basis. The digital governance approach should ensure the consistent application of essential governance mechanisms and operational process controls across all the segregated digital functions of the organisation. It should effectively resolve the following problems, in order to achieve the above: 1) the ever increasing size and complexity of the IT and control systems landscape and asset data (big data); 2) the isolation of the control systems and incompatible digital technology; 3) information security threats, due to the integration of the IT and control system landscapes; 4) inadequate digital governance of control system environments and the inconsistent maturity of digital governance between the IT and control system environments; and 5) inadequate assurance, due to following a pure compliance objective for digital governance (Chapter 4).

2. ***What is the appropriate approach to implement enterprise-wide digital governance in a sustainable manner for a large, traditional, complex, heterogeneous asset intensive organisation?***

   The objective of this research question is to determine the appropriate way of introducing and implementing the new way of thinking, working, controlling and modelling in a manner that is effective and sustainable. The new way of thinking should be: 1) accepted by all the digital functions of the organisation; and 2) embedded into the way of working of all the digital functions. Infrastructure asset management is typically practiced in infrastructure asset intensive, or industrial, organisations. These organisations are normally large and complex. Both IT and control systems are typically found in such organisations. This implementation approach should address the related problems, such as the organisational segregation of IT and control system functions in large and complex infrastructure asset intensive organisations, that could lead to: 1) a lack of knowledge

sharing, involvement and collaboration; 2) unclear roles and responsibilities; 3) a lack of trust between the digital functions; and 4) resistance to the new way of thinking and working (Chapter 4).

The problems resolved by the Rand Water Way are ***general real-world problems of infrastructure asset intensive organisations***. It was observed during the literature review that the problems extracted from the base case are not unique to Rand Water (Chapter 4). They are adequately reflected in literature. This includes literature on infrastructure asset management, decision making, digital technology, enterprise architecture, information management, and organisational change management, and transition management (Chapters 2 & 4). This was an indication that the artefact designed and instantiated at Rand Water, could potentially also add value to other similar organisations with similar problems. This includes infrastructure asset intensive organisations outside of the water and sanitation industry. This theory was subsequently tested when the Rand Water Way was evaluated (Chapter 7 and Annexure B). The result of the problem relevance section of the evaluation showed that all nine of the organisations who participated in the evaluation, were of the opinion that the majority of the problems being addressed by the Rand Water Way are also relevant to their respective organisations (Chapter 7 and Annexure B).

8.2. Research Rigour

Research methods must be rigorously applied and the presentation of results needs to address the rigour requirements of the academic audience (Hevner, March, Park & Ram, 2004).

This research applied a recognised, appropriate and ***rigorous research approach*** (Chapter 1). The researcher is a reflective practitioner, whose reflections induced the artefact (i.e. the Rand Water Way) that was designed for, and instantiated at, the base case. A design science research philosophy was followed, in order to create and apply an innovative artefact (Chapters 5 & 6) that will solve real world problems (Chapters 1 & 4) and acquire knowledge and understanding of the associated problem domain and the solution to the problems (Chapters 4 & 5) *(Hevner & Chatterjee, 2010).* Pragmatism was adopted as the epistemological stance for the research to ensure that The Rand Water Way is useful in practice *(March & Smith. 1995).* This research used the inductive-hypothetic research strategy to formulate and test a tentative hypothesis (i.e. the Rand Water Way design) *(Gonzalez & Sol, 2012).* This research strategy combines

theory and practice, by ensuring that the Rand Water Way is shaped by the organisational context. The Rand Water Way was described using the "ways of" framework of Seligmann *(1989).* The acceptance of the Rand Water Way was tested, by illustrating its usage, as well as evaluating its perceived usefulness and usability *(Keen & Sol, 2008; Davis, 1989).* It was evaluated at the base case, Rand Water, and at nine similar organisations in the mining, water, logistics and manufacturing industries (Chapters 6 & 7 and Annexure B). Several appropriate and recognised research instruments were used. The instruments included: 1) literature reviews; 2) interviews with expert panel members and questionnaires for the evaluation of the Rand Water Way; and 3) case studies *(Neuman, 2003; Johnson & Turner, 2003; Darke, Shanks & Broadbent, 1998).* Multiple case studies were used to examine the Rand Water Way in its real-life context, namely infrastructure asset intensive organisations (Chapters 3 & 7) *(Yin, 2003).* This included Rand Water, as the base case of the research (Chapters 3 and 6).

8.3. Artefact Evaluation and Acceptance

> *The utility, quality and efficacy of the design artefact must be rigorously evaluated via a well-executed evaluation method* (Hevner, March, Park & Ram, 2004; Gregor & Hevner, 2013). *The acceptance of the artefact must be tested by evaluating its perceived usefulness and usability* (Davis, 1989). *The artefact also needs to be operationalised and used in practice, for it to be successful and "measureable"* (Gonzalez & Sol, 2012).

The Rand Water Way was ***operationalised and is used in practice*** at Rand Water. The Rand Water Way was instantiated by: 1) contextualising it based on the Rand Water characteristics; 2) obtaining acceptance and approval from the authorised governance structures; and 3) implementing it across the three digital functions of the organisation (Chapter 6). Rand Water ***received value*** from the instantiation of the Rand Water Way. A number of the security related incidents, that occurred prior to the implementation of the Rand Water Way, seized to occur after the implementation. Examples of such incidents are: 1) the failure of the digital network and system integration solution, due to uncontrolled changes to the network and SCADA system; and 2) malicious software originating from SCADA servers that attempted to infect the IT environment (Chapters 6). As a result, Rand Water is now able to integrate and utilise quality asset information from both the IT and control systems on a continuous basis and in a safe and secure manner for the purpose of evidence-based strategic infrastructure asset management decision making (Chapters 6 & 7). Asset information from across the digital

landscape is therefore being managed as an enterprise resource. Rand Water is also now able to achieve wide area network related cost savings by exploiting the convergence in digital technology in a safe and secure manner (Chapter 6). In addition, the three previously isolated digital functions of the organisation are now: 1) involved in the digital governance structures; 2) complying with enterprise-wide operational process controls: and 3) collaborating and communicating with each other, to resolve common problems and achieve common objectives (Chapters 6 & 7).

The ***acceptance of the Rand Water Way was tested by rigorously evaluating its perceived usefulness and usability, via a well-executed evaluation method.*** The acceptance of the Rand Water Way was tested at Rand Water by evaluating it as an instantiated artefact. Representatives from the three digital functions and the infrastructure asset management function of Rand Water were included on the expert panel. This ensured that an enterprise-wide and unbiased opinion could be obtained. The 37 evaluation criteria were based on the requirements of the artefact. These requirements were in turn based on the problems that needed to be resolved (Chapters 4 & 7). The evaluation therefore tested whether the problems described in Chapter 4 have been resolved by the Rand Water Way, based on the perception or opinion of the expert panel members. The acceptance of the Rand Water Way was also tested at other similar organisations. The potential usefulness and usability of a contextualised Rand Water Way were evaluated. This evaluation utilised the same evaluation criteria and research instruments that were utilised for the Rand Water evaluation (Chapter 7 and Annexure B). The panel of experts represented organisations from the mining, water, manufacturing and logistics industries. The evaluation therefore tested the degree of generalisability of the Rand Water Way, by evaluating whether it could potentially provide value to infrastructure asset intensive organisations across different industries. The majority of the participating organisations were larger and more complex than Rand Water. The evaluation therefore also tested the acceptance of the Rand Water Way by organisations that were at least as large and complex as Rand Water.

The ***results of the evaluation*** at Rand Water and at the similar organisations were positive. The results showed that: 1) the problems originally extracted from the base case and generalised from literature, are prevalent at large and complex infrastructure asset intensive organisations across different industries; 2) the Rand Water Way is useful to Rand Water, because it effectively addressed their problems; 3) the Rand Water Way has been adequately generalised, in order for a contextualised version to potentially be useful to large and complex infrastructure asset intensive organisations across different industries; and 4) the Rand Water Way is “easy

to use" by, and appropriate for, asset intensive organisations across different industries. The Rand Water Way satisfied the requirements defined for the artefact (Chapter 4) and provided answers to the research questions (Chapter 1).

8.4. Research Contribution

> *Design science should create and apply an innovative artefact to acquire knowledge and understanding of the problem domain and the solution* (March & Smith, 1995; Hevner & Chatterjee, 2010). *This includes both descriptive and prescriptive knowledge* (Gregor & Hevner, 2013). *The contribution of the research should be seen to arise out of the novelty, generality and significance of the design artefact* (Hevner, March, Park & Ram, 2004). *The contribution includes the design artefact itself, as well as new constructs, models and instantiations* (Hevner, March, Park & Ram, 2004). *Design science research must also contribute to theory* (Alturki & Gable, 2014).

The research ***contributes indirectly to society***. The lack of timely infrastructure investment and poorly performing infrastructure assets, including critical national installations, have a significant negative impact on society (Chapter 1). This negative impact includes the lack of economic growth, the decrease in quality of life of citizens, and loss of life. The improvement in infrastructure asset management, via improved strategic asset management decision making, will make a direct positive contribution to society. The aim of the research is to improve the management of asset information at an enterprise level through enterprise digital governance. This will improve and enable effective strategic infrastructure asset management decision making.

The research contributes to ***descriptive knowledge by increasing the knowledge and understanding of:*** 1) the associated problem domain; and 2) the related concepts and theories. The knowledge and understanding of the problem domain is increased by describing the problems related to the research topic. These include the problems extracted from the base case and found in literature (Chapter 4). The research also increases knowledge regarding the common nature of the problems being experienced by infrastructure asset intensive organisations across different industries, such as the water, mining, manufacturing and logistics industries. This was initially observed during the literature reviews (Chapter 4) and was thereafter confirmed during the evaluation of the Rand Water Way (Chapter 7). The research described the relevant concepts and disciplines related to the problem domain and research

topic (Chapter 2). These concepts and disciplines include asset management, decision making, enterprise architecture, information management, digital technology convergence, IT governance, change management, and transition management. The research also described the trends and observations regarding those disciplines that are relevant to the research topic and that influenced the design of the artefact. The research further illustrated the gap in the literature and knowledge regarding: 1) digital governance in control system environments; 2) enterprise-wide digital governance for industrial organisations, that applies to both IT and control system environments; and 3) an approach to implement enterprise-wide digital governance in a large complex infrastructure asset intensive organisation (Chapters 2 & 4).

The research contributes to ***prescriptive knowledge,*** as well as ***science and theory,*** through the ***design and instantiation of an identifiable novel artefact with high utility***, namely the Rand Water Way. It addresses the gap in literature mentioned above. The research contributes to the fields and theory of information management and digital governance, as applied to large and complex infrastructure asset intensive organisations. The research provides answers to the two research questions posed by the research (Chapter 1) by: 1) defining an appropriate enterprise-wide digital governance approach that enables effective strategic infrastructure asset management decision making, via improved enterprise-wide asset information management; and 2) defining an appropriate transition management approach for implementing the new way of thinking, working, controlling and modelling in a large and complex infrastructure asset intensive organisation (Chapters 5 and Annexure A).

The Rand Water Way is a ***unique artefact.*** No similar approach could be found in literature (Chapter 2). To the researcher's knowledge, this is the first attempt to: 1) address these research questions; and 2) design, instantiate and evaluate an approach that addresses the asset information management problems of large and complex infrastructure asset intensive organisations. The Rand Water Way is based on accepted theories, concepts and trends from literature regarding a range of related disciplines (e.g. enterprise architecture, information management, IT governance) (Chapter 2). The uniqueness of the Rand Water Way is primarily found in: 1) the integration and encapsulation of these individual concepts and theories into a single integrated approach; and 2) the application of these theories to the topic of digital governance, in support of strategic infrastructure asset management decision making in large and complex infrastructure asset intensive organisations. Each of the integrated constituent parts of the Rand Water Way are required to make its own unique contribution to the holistic and collective solution to the problems.

Some of the unique characteristics of the Rand Water Way are (Chapter 5 & Annexure A):

Unique Characteristic	Description
Integrated enterprise-wide approach that includes IT and control systems	The Rand Water Way goes beyond IT governance, IT management and information management. It addresses digital governance in an integrated manner at an enterprise-level, by including both the IT and control system environments of an infrastructure asset intensive organisation. The scope of the strategy, architecture and information management constituent parts of the Rand Water Way were also extended, from the typical IT scope found in literature, to include both the IT and control system environments.
Balanced digital governance using a risk-based two tier prioritisation hierarchy	The Rand Water Way goes beyond compliance to any specific standard, code or framework. It provides an appropriate balanced ("just enough") approach to digital governance, that includes a risk-based prioritisation of both digital governance mechanisms and operational process controls. The digital governance constituent part of the Rand Water Way includes a unique digital governance mechanism and operational process control prioritisation method and presentation. It is a two-tier hierarchy consisting of: Tier 1 - essential centralised controls; and Tier 2 - important federated controls.
Adaptable transition roadmap with continuous phases that focuses on trust building before formalisation	The Rand Water Way includes a transition management approach that is appropriate to introduce and embed the new way of digital governance in a large complex infrastructure asset intensive organisation. It includes a unique transition roadmap that is adequately flexible and adaptable to cater for: 1) a tailored solution based on the characteristics of an organisation; 2) changes to the organisation; and 3) responding to short-term improvement opportunities. The roadmap includes phases and stages that are continuous in nature, instead of a typical "step ladder" approach to improving maturity. It firstly focuses on building trust between the digital functions. Thereafter it focuses on achieving efficiency related improvements to illustrate value in a manner that limits the residual risk to an acceptable level. Finally, the focus moves to the formalisation of the digital environment (e.g. architecture, strategy, governance).

Table 8-1 Unique Characteristics of the Rand Water Way

These unique characteristics of the Rand Water Way ensure that the implementation of digital governance across the IT and control system environments adheres to some of the key IT governance objectives, namely: 1) value delivery; 2) risk management; and 3) sustaining the organisation's objectives by balancing risk and value (Chapter 2).

The research ***contributes to theory*** via the Rand Water Way design and instantiation. These theories are based on, and are in line with, the above mentioned unique characteristics of the Rand Water Way. Some of the primary theories encapsulated and embodied by the Rand Water Way are:

Theory	Theory Description and Explanation
An integrated enterprise-wide approach for asset information management is required to enable infrastructure asset management decision making.	An approach that will successfully enable asset information management in support of strategic infrastructure asset management decision making requires: 1) The enterprise-wide management of digital information from IT and control systems as a valuable enterprise resource; 2) A strategy that drives the rest of the constituent parts of the approach and ensures acceptance of, and commitment to, the approach; 3) An enterprise architecture and related standards that include IT and control systems; 4) The enterprise-wide governance of the digital environment, including IT and control systems; 5) Compliance by all of the digital functions and projects of the organisation; 6) A transition management approach to implement the new way of thinking and working in a sustainable manner; and 7) The collective contribution by each of the constituent parts of the approach, to holistically and effectively resolve the associated problems.
A single enterprise-wide view of digital technology and asset information is required to enable infrastructure asset management decision making.	The digital technology landscape and asset information should be viewed, managed and governed as a single enterprise-wide landscape and resource, in order to effectively support strategic infrastructure asset decision making. This includes the following: 1) The IT and control system landscapes should be thought of and managed as one single integrated digital technology landscape; 2) The asset data originating from the IT and control systems landscapes should be thought of as a single critical enterprise resources; and 3) The security threats to the IT and control systems landscapes should be viewed and mitigated as a common threat that requires a combined response.
A continuous work stream with quick wins to achieve a legitimate vision is required to successfully implement the new way of digital governance.	An approach that will successfully achieve the desired digital governance future state or target maturity level at an infrastructure asset intensive organisation should: 1) Have a legitimate longer term vision and journey that is agreed to by all the digital functions of the organisation; 2) Achieve quick wins with acceptable residual risk to maintain the momentum and to exploit short term improvement opportunities; and 3) View the stages of the roadmap as continuous work streams to improve digital governance maturity, rather than a typical “step ladder” approach.

Theory	Theory Description and Explanation
A balanced "just enough" digital governance approach using risk-based controls prioritisation is required to optimise risk and cost, as well as to ensure acceptance of the new way of digital governance within an infrastructure asset intensive organisation.	An appropriate balanced ("just enough") risk-based digital governance approach for both governance mechanisms and operational process controls will: 1) Adequately mitigate the risks for an infrastructure asset intensive organisation that wants to integrate its IT and control system environments; 2) Resolve the associated problems experienced in terms of collecting and delivering quality harmonised asset data for effective infrastructure asset decision making; 3) Provide a cost effective and efficient digital governance solution by avoiding the pitfalls of over-regulation; 4) Provide clarity in terms of decision making authority, roles and responsibilities of the segregated digital functions; and 5) Be acceptable to the IT and control system functions of an infrastructure asset intensive organisation, because it delivers value, whilst providing the digital functions with enough freedom to make operational decisions. This is based on the principle that the higher the risk due to the absence of a control: 1) the higher the level of criticality of that control; 2) the higher the degree of centralisation and regulation required regarding that control; and 3) the lower the degree of flexibility and autonomy of the digital functions in relation to that control.
Trust-based collaboration with commitment and involvement from all digital functions is required to ensure acceptance and the sustainability of the new way of digital governance within an infrastructure asset intensive organisation.	An approach that will successfully introduce the new way of thinking to, and embed the new way of working in, an infrastructure asset intensive organisation should: 1) Build trust between the digital functions of the organisation before attempting to: 1) obtain formal longer term commitment from the digital functions; 2) formalise the relationship between the digital functions; or 3) propose high risk collaboration or digital shared service initiatives; 2) Include all digital functions in the governance structures and utilise these structures as engagement and change forums; 3) Provide the digital function proposing the change with adequate legitimacy, by ensuring that it implements the governance mechanisms and controls within its own area of responsibility, before requesting any other digital function to do the same (i.e. bedrock factors); 4) Define and agree on the digital organisational structure as soon as possible in the transition journey (e.g. centralisation, federation, decentralisation), in order to reduce uncertainty and improve the commitment from all the affected digital functions; 5) Include elements of organisational change management in the transition roadmap itself, rather than treating it as a separate isolated supporting work stream; and 6) Recognise that the role of the digital functions will change over time (i.e. IT customer, business partner, governance stakeholder), as the required commitment from all digital functions increases and the degree of formalisation increases.

Table 8-2 Theories Encapsulated by the Rand Water Way

The theories listed above primarily address: 1) how digital technology and information should be viewed, managed and governed, in order to support infrastructure asset management; and

2) the required characteristics of an approach to successfully implement this new way in a large, complex, infrastructure asset organisation.

The Rand Water Way ***instantiation at the base case*** also contributes to the fields of information management, digital governance and transition management at a ***practical level***. It increases the ***prescriptive knowledge*** about how such a new way of thinking, working, controlling and modelling can be successfully contextualised for, introduced to, and embedded into a large complex infrastructure asset intensive organisation, such as Rand Water, in a manner that is sustainable and adds value to the organisation (Chapters 6).

8.5. Direction for Further Research

This research creates an avenue for further research related to infrastructure asset management decision making and digital governance in infrastructure asset intensive organisations. The following are examples of possible further research related to this research topic:

1) The adaptation, contextualisation and instantiation of the Rand Water Way to address the asset information management and digital governance related problems experienced by multi-national organisations with autonomous or semi-autonomous business units or legal entities, each with its own infrastructure installations;

2) The design and instantiation of an infrastructure asset management decision enhancement studio, focusing on strategic infrastructure asset management decisions for large and complex infrastructure asset intensive organisations, enabled by the Rand Water Way as a foundation;

3) Determining and assessing the state and maturity of digital governance for control system environments of infrastructure asset intensive organisations globally, based on empirical evidence;

4) The incorporation of less structured information or tacit knowledge, such as political and social considerations, into the information base for supporting effective strategic infrastructure asset management decision making; and

5) The adaptation, contextualisation and instantiation of the Rand Water Way for other core strategic business decisions of industrial or infrastructure asset intensive organisations, such as product quality management decisions or operational (e.g. manufacturing) process efficiency improvement decisions.

References

Agievich, V. & Skripkin, K. (2014). *Enterprise architecture migration planning using the matrix change. Procedia Computer Science. 31. Pages 231-235.*

Ahmad, A., Hadgkiss, J. & Ruighaver, A.B. (2012). *Incident response teams – challenges in supporting the organisational security function. Computer & Security. 31. Pages 643-652.*

Alturki, A. & Gable, G.G. (2014). *Theorizing in Design Science Research: An Abstraction Layers Framework. PACIS 2014 Proceedings. Paper 126.*

American Society of Civil Engineers. (2013). *Report card for America's infrastructure. April 2013, Pittsburgh.*

American Water Works Association. (2002). *Assessing the future – Water utility infrastructure management.*

American Water Works Association. (2003). *The evolving water utility.*

Anderson, D. & Anderson, L.A. (2001). *Beyond change management. ISBN 0-7879-5645-7.*

Anwar, A. & Mahmood, A.N. (2014). *Cyber security of the smart grid. The state of the art in intrusion prevention and detection. Pages 449-472.*

Association of Information and Imaging Management. (2014). *Enterprise content management glossary.*

Augustine, N.R. (1998). *Reshaping an industry: Lockheed Martin's survival*. *Harvard Business Review on Change. Pages 159-188. ISBN 0-87584-844-2.*

Aversano, L., Grasso, C. & Tortorella, M. (2012). *A literature review of business/IT alignment strategies. Procedia Technology. 5. Pages 462-474.*

Becker, J., Knackstedt, R. & Pöppelbuß, J. (2009). *Developing maturity models for IT management – a procedure model and its application. Business & Information Systems Engineering. 1. Pages 204-213.*

Benaroch, M, Chernobai, A. & Goldstein, J. (2012). *An internal control perspective on the market value consequences of IT operational risk events. International Journal of Accounting Information Systems. 13. Pages 357-381.*

Bowen, P.L., Chung, M.D. & Rohde, F.H. (2007). *Enhancing IT governance practices: A model and case study of an organisation's efforts. International Journal of Accounting Information Systems. 8. Pages 191-221.*

BSI - British Standards Institute. (2003). *Managing culture and knowledge: Guide to good practice.*

Burns, P. (2010). *Asset management strategy: Leadership and decision-making. Whole-life management of physical assets. Pages 94-115. ISBN: 798-0-7277-3653-6.*

Byrd, T.A., Lewis, B. & Bryan, R.W. (2006). *The leveraging influence of strategic alignment on IT investment: An empirical examination. Information & Management. 43. Pages 308-321.*

Caldwell, T., Maude, J. & Gallego, R. (2015). *Hacktivism goes hard core. Network Security. 5. Pages 12-17.*

Campbell, R.J. (2011). *The smart grid and cyber security – Regulatory policy issues. Congressional research service – Report for Congress. www.crs.gov.*

Chang, R.M., Kauffman, R.J. & Kwon, Y. (2014). *Understanding the paradigm shift to computational social science in the presence of big data. Decision Support Systems. 63. Pages 67–80. Singapore Management University.*

Charoensuk, S., Wongsurawat, W. & Kang, D.B. (2014). *Business-IT alignment: A practical approach. Journal of High Technology Management Research. 25. Pages 132-147.*

Chen, C.L.P & Zhang, C.Y. (2014). *Data-intensive applications, challenges, techniques and technologies: A survey on big data. Information Sciences. 275. Pages 314–347. University of Macau.*

Chitambala, G. (2006). *Status of IT Governance in South Africa: A comparative view: Gordon Institute of Business Science – University of Pretoria.*

Clarke, S. (2006). *The relationship between safety climate and safety performance. Journal of Occupational Health Psychology. 11 (4). Pages 315-327.*

Collins, J.C. & Porras, J.I. (1998). *Building your company's vision. Harvard Business Review on Change. Pages 21-54. ISBN 0-87584-844-2.*

Colwill, C. (2009). *Human factors in information security: the insider threat – who can you trust these days? Information Security Technology Report. 14 (4). Pages 186-196.*

Conger, J.A, Spreitzer, G.M. & Lawler, E.E. (1999). *The leader's change handbook: An essential guide to setting direction and taking action. Jossey-Bass. San Francisco, CA.*

COSO - Committee of Sponsoring Organisations. *(2004). Enterprise risk management - integrated framework.*

Costella, S.B., Chapman, D.N., Rogers, C.D.F. & Metje, N. (2007). *Underground asset location and condition assessment technologies. Tunnelling and Underground Space Technology. 22. Pages 524-542.*

Darke, P., Shanks, G. & Broadbent, M. (1998). *Successfully completing case study research: Combining rigor, relevance and pragmatism. Information Systems Journal. 8. Pages 273-289.*

Davis, F.D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly. Management Information Systems. 13 (3). Pages 319-340.*

de Vreede, G. & Briggs, R.O. (2005). *Collaboration engineering: Designing repeatable processes for high-value collaborative tasks: Proceedings of the 38th Hawaii international conference on systems design.*

Department of Public Service and Administration: Republic of South Africa. (2012). *Corporate governance of ICT policy framework.*

Department of Public Works: Republic of South Africa. (2006). *National infrastructure maintenance strategy.*

Dhami, M.K. & Thomson, M.E. (2012). *On the relevance of cognitive continuum theory and quasirationality for understanding management judgement and decision making. European Management Journal. 30. Pages 316-326. University of Glascow.*

Douglas, C.C. (2014). *An open framework for dynamic big-data-driven application systems (DBDDAS) development. ICCS 2014. 14th International conference on computational science. 29. Pages 1246–1255.*

Duck, J.D. (1998). *Managing change: The art of balancing. Harvard Business Review on Change. Pages 55-82. ISBN 0-87584-844-2.*

Duhigg, C. (2009). *Millions in U.S. drink dirty water, records show. The New York Times.*

East, N. (2011). *Implement an effective change management strategy. ISBN 978-1-907787-86-7.*

Edwards, R. (2010). *Asset management in the rail and utilities sector. Whole-life management of physical assets. Pages 3-26. ISBN: 798-0-7277-3653-6.*

European KM Forum. (2002). *KM Framework - 2nd release.*

Federal Energy Regulatory Commission. (2013). *Assessment of demand and advanced metering staff report 2013.*

Feng, N., Wang, J. & Li, M. (2014). *A security risk analysis model for information systems: Casual relationships of risk factors and vulnerability propagation analysis. Information Sciences. 256. Pages 57-73.*

Fernández-de-Alba, J.M., Fuentes-Fernández, R. & Pavón, J. (2013). *Architecture for management and fusion of context information. Information Fusion. 21. Pages 100-113.*

Flores, W.R., Antonsen, E. & Ekstedt, M. (2014). *Information security knowledge sharing in organisations: Investigating the effect of behavioural information security governance on national culture. Computers & Security. 43. Pages 90-110.*

Fonstad, N. & Robertson, D. (2004). *Realizing IT-enabled change: The IT engagement model. Sloan School of Management – Massachusetts Institute of Technology. 4 (3D). October 2004.*

Fuchs, L., Pernul, G. & Sandhu, R. (2011). *Roles in information security – A survey and classification of the research area. Computers & Security. 30. Pages 748-769.*

Gartner. *(2013). 2014 Strategic road map for IT/OT alignment.*

Georghiou, L. & Keenan, M. (2006). *Evaluation of national foresight activities: Assessing rationale, process and impact. Technology Forecasting and Social Change. 73. Pages 761-777.*

Geum, Y., Lee, S. & Park, Y. (2014). *Combining technology roadmap and system dynamics simulation to support scenario-planning: A case of car-sharing service. Computers & Industrial Engineering. 71. Pages 37–49.*

Gheorghe, M. (2010). *Audit methodology for IT governance. Informatica Economică. 14 (1). Pages 32-42.*

Giachetti, R.E. (2012). *A flexible approach to realize an enterprise architecture. Procedia Computer Science. 8. Pages 147-152.*

Global Forum on Maintenance and Asset Management. (2011). *The asset management landscape – 2nd edition. ISBN 978-0-9871799-2-0.*

Global Water Intelligence. (2013). *Smart water networks.*

Gonzalez, R.A. & Sol, H.G. (2012). *Validation and design science research in information systems. In Mora, M., Gelman, O., Steenkamp, A.L., & Raisinghani, M. (Eds). Research methodologies, innovations and philosophies in software systems engineering and information system. IGI Global. Pages 403-426.*

Gonzalez, R.A. (2010). *A framework for ICT support coordination in crisis response. Doctoral dissertation: Delft University of Technology.*

Goss, T., Pascale, R. & Athos, A. (1998). *The reinvention roller coaster: Risking the present for a powerful future. Harvard Business Review on Change. Pages 83-112. ISBN 0-87584-844-2.*

Gregor, S. and Hevner, A.R. (2013). *Positioning and presenting design science research for maximum impact: Research essay. MSI Quarterly, 37 (2, June), Pages 1-6.*

Haday, P. & Cassivi, L. (2012). *Joint collaborative planning as a governance mechanism to strengthen the chain of IT value co-creation. Journal of Strategic Information Systems. 21. Pages 182-200.*

Hammoudech, M. & Newman, R. (2013). *Information extraction from sensor networks using the Watershed transform algorithm. Information Fusion. 22. Pages 39-49.*

Hevner, A., March, S., Park, J. & Ram, S. (2004). *Design science in information research. MIS Quarterly. 28. Pages 75-105.*

Hevner, H.R. & Chatterjee, S. (2010). *Design research in information research: Theory and practice. New York Dordrecht Heidelberg London: Springer.*

Huard, B. (2015). *The data quality paradox. Network Security. 6. Pages 18-20.*

Humphrey, W. (1989). *Managing the software process.*

Institute of Asset Management. (2008). *PAS 55-1:2008 Asset Management – Part 1: Specification for the optimized management of physical assets. ISBN 978-0-580-50975-9.*

Institute of Directors of South Africa. (2009). *King code of good governance for South Africa: King III.*

Institute of Public Works Australia. (2011). *International infrastructure asset management manual - 2011 edition. ISBN 0-473-10685-7.*

International Road Transport Union. (2009). *Road transport in the People's Republic of China. Geneva.*

ISACA. (2011). *Certified in the governance of enterprise IT review manual.*

ISACA. (2012). *2012 Governance of enterprise IT survey - global edition.*

ISO - International Standards Organisation. (2001). *ISO 15489: Information and documentation – Records management – Part 1: General.*

ISO - International Standards Organisation. (2008). *ISO 38500: Corporate governance of information technology.*

ISO - International Standards Organisation. (2008). *ISO 42010: Systems and software engineering – Recommended practice for architectural description of software-intensive systems.*

ISO - International Standards Organisation. (2014). *ISO 55000: Asset management – Overview, principles and technology – 1st edition.*

ISO - International Standards Organisation. (2005). *ISO 27001: Information technology – Security techniques – Information security management system – Requirements.*

IT Governance Institute. (2007). *COBIT 4.1 - 4th edition*

IT Governance Institute. (2011). *Global status report on the governance of enterprise IT – 2011.*

IT Governance Institute. (2012). *COBIT 5.1 – A business framework for the governance and management of enterprise IT. ISBN 978-1-60420-237-3.*

Iyamu, T. (2011). *The architecture of information in organisations. SA Journal of Information Management. 13 (1). Art # 419. Pages 1-9.*

Jaatun, M.G., Røstum, S. Peterson, S. & Ugarelli, R. (2014). *Security checklists: A compliance alibi, or a useful tool for water network operators?. Procedia Engineering. 70. Pages 872-876. 12th International conference on computing and control for the water industry, CCWI2013.*

Jamieson, S. (2004). *Likert Scales: How to (ab)use them. Medical education. 38 (12). Pages 1217-1218.*

Johnson, B. and Turner, L.A. (2003). *Data collection strategies in mixed methods research. In A. Tashakkon & C. Teddlie (Eds.). Handbook of mixed methods in social and behavioural research. Pages 297-320. USA: Sage Publications, Inc.*

Johnson, C. (2010). *Creating an asset management culture. Whole-life management of physical assets. Pages 116-137. ISBN: 798-0-7277-3653-6.*

Jouine, M., Arfa, L.B.A. & Aissa, A.B. (2014). *Classification of security threats in information systems. Procedia Computer Science. 32. Pages 489-496. 5th International conference on ambient systems. Networks and Technologies (ANT-2014).*

Kang, D., Lee, J. & Kim, K. (2010). *Alignment of business enterprise architectures using fact-based ontologies. Expert Systems with Applications. 37. Pages 3274-3283.*

Kang, D., Lee, J., Choi, S. & Kim, K. (2010). *An ontology enterprise architecture. Expert Systems with Applications. 37. Pages 1456-1464.*

Kaplan, J. (2005). *Strategic IT portfolio management: Governing enterprise transformation. USA: Pittiglio Rabin Todd and McGrath Inc.*

Kaplan, R.R & Norton, D.P. (2001). *The strategy-focused organisation. Harvard Business School. ISBN 1-57851-250-6.*

Keen, P.G.W. & Sol, H.G. (2008). *Decision Enhancement Services: Rehearsing the future of decisions that matter. ISBN 978-1-58603-837-3.*

Kerr, D.S & Murthy, U.S. (2013). *The importance of the CobiT framework IT processes for effective internal control over financial reporting in organisations: An international survey. Information & Management. 50. Pages 590-597.*

Kiameh, P. (2003). *Power generation handbook: Selection, applications, operation and maintenance. ISBN: 9780071396042*

King, K. & Knight, W. (2003). *Uninterruptible power supplies. ISBN: 9780071395953.*

Kluth, A., Jäger, J., Schatz, A. & Bauernhansl, T. (2014). *Evaluation of complexity management systems – Systematical and maturity-based approach. Variety management in manufacturing. Proceedings of the 47th CIRP conference on manufacturing systems. Procedia CIRP. 17. Pages 224 – 229.*

Kommission Zukunft der Verkehrsinfrastrukturfinanzierung. (2010*). Zukunft der verkehrsinfrastrukturfinanzierung. Berlin.*

Kooper, M.N., Maes, R., & Lindgreen, E.E.O. (2011). *On the governance of information: Introducing a new concept of governance to support the management of information. International Journal of Information Management. 31. Pages 195-200.*

Kotter, J. & Schlesinger, L.A. *(2008). Choosing strategies for change. Harvard Business Review. July – August 2008.*

Kotter, J. (1995). *Leading change: Why transformation effort fail. Harvard Business Review.*

Kotter, J. (2012). *The 8-step process for leading change.*

Kotter, J. (1998). *Leading change: Why transformation efforts fail. Harvard Business Review on Change. Pages 1-20. ISBN 0-87584-844-2.*

Kwon, O., Lee, N. & Shin, B. (2014). *Data quality management, data usage experience and acquisition intention of big data analytics. International Journal of Information Management. 34. Pages 387–394. Kyung Hee University.*

Kyriakidou, A., Michalakelis, C. & Sphicopoulos, T. (2013). *Assessment of information and communication technology maturity level. Telecommunications Policy. 37. Pages 48-62.*

Lange, L. & Kasan, H. (2014). *Paradigm shift from engineering to asset management: Rand Water, the largest water utility in Africa. Water Utility Management International, March 2014.*

Lau, H.C.W & Dwight, R.A. (2011). *A fuzzy-based decision support model for engineering asset condition monitoring – A case study examination of water pipelines. Expert Systems with Applications. 30. Pages 13342-13350.*

Lehman, M.C & Heagy, C.D. (2014). *Organizing information into useful management reports: Short cases to illustrate reporting principles and coding. Journal of Accounting Education. 32. Pages 130-145.*

Leitão, A., Cunha, P., Valente, F. & Marques, P. (2013). *Roadmap for business model definition in manufacturing companies. Procedia CIRP. 7. Pages 383-388.*

Leung, Y., Ji, N. & Ma, J. (2013). *An integrated information fusion approach based on the theory of evidence and group decision making. Information Fusion. 15. Pages 126-148. The Chinese University of Hong Kong.*

Liell-Cock, S., Graham, J. & Hill, P. (2009). *IT governance aligned to King III. IT Governance Network.*

Lloyd, C. (2012). *International case studies in asset management. ISBN 978-0-7277-5739-5*.

Lunardi, G.L., Becker, J.L., Maçada, A.C.G. & Dolci, P.C. (2014). *The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms. International Journal of Accounting Information Systems. 15. Pages 66-81*.

Macaulay, T. & Singer, B. (2012). *Cybersecurity for industrial control systems. ISBN 978-1-4398-0196-3.*

Madsen, M. (2013). *Disciplinary perspectives on information management. Procedia Social and Behavioral Sciences. 73. Pages 534-537.*

Male, S. (2010). *The challenges facing public sector asset management. Whole-life management of physical assets. Pages 50-73. ISBN: 798-0-7277-3653-6.*

Mamaghani, N.D., Madani, F.M. & Sharifi, A. (2012). *Customer oriented enterprise IT architecture framework. Telematics and Informatics. 29. Pages 219-232.*

Manganelli, R.L & Klein, M.M. (1994). *The re-engineering handbook: A step-by-step guide to business transformation. ISBN 0-8144-0236-4.*

March, S.T. & Smith, G.F. (1995). *Design and natural science research on information technology. Decision Support Systems. 15 (4). Pages 32-46.*

Martin, R. (1998). *Changing the mind of the corporation. Harvard Business Review on Change. Pages 113-128. ISBN 0-87584-844-2.*

Matrosov, E.S., Woods, A.M. & Harou, J.J. (2013). *Robust decision making and info-gap decision theory for water resource system planning. Journal of Hydrology. 9. Pages 43-58. University College London.*

Matwyshyn, A. (2009). *CSR and the corporate cyborg: Ethical corporate information security practices. Journal of Business Ethics. 88. Pages 494-579.*

McDowall, W. (2012). *Technology roadmaps for transition management: The case of hydrogen energy. Technology Forecasting & Social Change. 79. Pages 530-542.*

Mearns, K., Whitaker, S.M. & Flin, R. (2003). *Safety climate, safety management practices and safety performance in off-shore environment. Safety Science. 41. Pages 641-680.*

Mingers, J. (2004). *Real-izing Information Systems: Critical Realism as an underpinning philosophy for information systems. Information and Organisation. 14 (2). Pages 76-83.*

National Planning Commission - South African Government. (2011). *South African national development plan.*

National Treasury: Republic of South Africa. (2013). *National budget review.*

NEPAD - New Partnership for Africa Development. (2012). *Programme for infrastructure development in Africa (PIDA)*

Neuman, W. L. (2003). *Social research methods: Qualitative and quantitative approaches. USA: Pearson Education, Inc.*

Nfuka, E.N. & Rusu. L. (2010). *Critical success factors for effective IT governance in the public sector organisations in a developing country: The case of Tanzania. In 18th European conference on information systems. Paper 128.*

Nolan, R. & McFarlan, FW. (2005). *Information technology and board of directors. Harvard Business Review. October 2005. Pages 1-10.*

Oliviera, M.G. & Rozenfeld, H. (2010). *Integrating technology road mapping and portfolio management at the front-end of new product development. Technological Forecasting & Social Change. 7. Pages 1339–1354.*

Othman, M.F.F., Chan, T. & Foo, E. (2011). *IT governance adoption in Malaysia: A preliminary investigation. Australian conference on information systems (ACIS 2011). Paper 69.*

Parker, S.P. (1984). *Dictionary of engineering.*

Pidd, H. (2012). *India blackouts leave 700 million without power. The Guardian.*

Pilling, M. (2010). *Beyond BSI PAS 55 compliance. Whole-life management of physical assets. Pages 75-90. ISBN: 798-0-7277-3653-6.*

PMI - Project Management Institute. (2013). *A guide to the project management body of knowledge - 5th edition.*

Political Economy Research Institute. (2009). *How infrastructure investments support the U.S. economy: Employment, productivity and growth. May 2009, Amherst.*

Port, D. & Wilf, J. (2014). *The value proposition for assurance of JPL systems. Procedia. 28. Pages 398-403. Conference of systems engineering research (CESR 2014).*

Pragma & Aurecon. (2012). *Asset management improvement plan (AMIP) framework.*

Prasad, A., Green, P. & Heales, J. (2012). *On IT governance structures and their effectiveness in collaborative organisational structures. International Journal of Accounting Information Systems. 13. Pages 199-220.*

Prasad, A., Heales, J. & Green, P. (2010). *A capabilities-based approach to obtaining a deeper understanding of information technology governance effectiveness: Evidence from IT steering committees. International Journal of Accounting Information Systems. 11. Pages 214-323.*

Presidential Infrastructure Coordinating Commission - South African Government. (2012). *South Africa national infrastructure Plan.*

Pulkkinen, M., Naumenko, A. & Luostarinen, K. (2007). *Managing information security in a business network of machinery maintenance services business – Enterprise architecture as a coordinating tool. The Journal of Systems and Software. 80. Pages 1607 – 1620.*

Rand Water. (2003). *100 years of excellence – 1903-2003. ISBN 0-620-32313-2*

Rand Water. (2013). *Integrated annual report 2012-3.*

Rand Water. *(2014). Integrated annual report 2013-4.*

Rasmussen, J. & Goodstein, L.P. (1987). *Decision support in supervisory control of high-risk industrial systems. Automation. 23 (5). Pages 663 – 671.*

Raval, V. & Dyche, D. (2012). *Seven myths of information governance. ISACA Journal. 4. Pages 1 – 6.*

Rayner, R. (2010). *Incorporating climate change within asset management. Whole-life management of physical assets. Pages 161-180. ISBN: 798-0-7277-3653-6.*

Rice, E.B & Almajali, A. (2014). *Mitigating the risk of cyber-attack on smart grid systems. Procedia computer science. 28. Pages 575-582. 2014 conference on systems engineering research.*

Romp, W. & de Haan, J. (2005). *Public and economic growth: A critical survey. European Investment Bank Papers. 10 (1). Pages 40-70.*

Rorty, R. (1999). *Philosophy and social hope, London: Penguin.*

Ross, J. (2004). *Generating strategic benefits from enterprise architecture. Sloan School of Management – Massachusetts Institute of Technology. 4 (3A). October 2004.*

Sambamurthy, V. & Zmud, R.W. (1999). *Arrangements for information technology governance: a theory of multiple contingencies. MIS Quarterly. 23. Pages 261-290.*

Šaša, A. & Krisper, M. (2011). *Enterprise architecture patterns for business process support analysis. The Journal of Systems and Software. 84. Pages 1480-1506.*

Schaffer, R.H. & Thomson, H.A. (1998). *Successful change programs begin with results. Harvard Business Review on change. Pages 189-214. ISBN 0-87584-884-2.*

Schawrtz, A. & Hirschheim, R. (2003). *An extended platform logic perspective of IT governance: Managing perceptions and activities of IT. Journal of Strategic Information Systems. 12(2). Pages 129-166.*

Seligmann, P.S., Wijers, G.M. & Sol, H.G. (1989). *Analysing the structures of IS methodologies: Proceedings of the 1st Dutch conference on information systems. Amersfoort, the Netherlands.*

Shamala, P., Ahmad, R. & Yusoff, M. (2013). *A conceptual framework of information structure for information security risk assessment. Journal of Information Security and Applications. 18. Pages 45-52.*

Shariati, M., Bahman, F. & Shams, F. (2011). *Enterprise information security – A review of architectures and frameworks from interoperability perspective. Procedia Computer Science. 3. Pages 537-543.*

Shedden, P., Ruighaver, A.B. & Ahmad, A. (2010). *Risk management standards – the perception of ease of use. Journal of Information Systems Security. 6 (3). Pages 23-41.*

Shedden, P., Scheepers, R., Smith, W. & Atif, A. (2011). *Incorporating a knowledge perspective into security risk assessments. Journal of Information and Knowledge Management Systems. 41 (2). Pages 152-175.*

Sheperd, E., Stevenson, A. & Flinn, A. (2010). *Information governance, records management, and freedom of information: A study of local government authorities in England. Government Information Quarterly. 27. Pages 337-345.*

Silva, M.M, de Gusmão, A.P.H., Poleto, T., e Silva, C.L. & Costa, A.P.C.S. (2014). *A multidimensional approach to information security risk management using FMEA and fuzzy theory. International Journal of Information Management. 34. Pages 733-740.*

Sirkin, L., Keenan, P. & Jackson, A. (2005). *The hard side of change management. Harvard Business Review.*

Sol, H.G. (1982). *Simulation in information systems development. Doctoral dissertation: University of Groningen.*

Soloman, S. (2010). *Sensors and control systems in manufacturing – 2nd edition. ISBN: 9780071605724.*

South African Institute of Civil Engineers. (2011). *Infrastructure report card for South Africa – 2011. www.saice.org.za.*

Spears, J.L., Barki, H & Barton, R.R. (2013). *Theorizing the concept and role of assurance in information system security. Information & Management. 50. Pages 598-605.*

Statistics South Africa. (2011). *Census 2011 Statistical release – P0301.4.*

Steensen, E.F. (2014). *Five types of organisational strategy. Scandinavian Journal of Management. 30. Pages 266-281.*

Stern, N. (2007). *The economics of climate change: The Stern Review. HM Treasury London.*

Strebel, P. (1998). *Why do employees resist change?. Harvard Business Review on Change. Pages 139-158. ISBN 0-87584-844-2.*

Suaro, J. & Lewis, J.R. (2011). *When designing usability questionnaires. Does it hurt to be positive? Proceedings of the international conference on human factors in computing systems (CHI). Pages 2215-2224.*

Swiss Re. (2009). *Natural catastrophes and man-made disasters in 2008, Sigma report 2/2009. Swiss Reinsurance Company. Zurich.*

The International Bank for Reconstruction and Development & World Bank. (2010). *Africa's infrastructure: A time for transformation. Washington DC.*

The IT Service Management Forum. (2013). *itSMF 2013 global survey on IT service management.*

The Open Group. (2009). *The Open Group architecture framework (TOGAF) - version 9. ISBN: 978-90-8753-230-7.*

The Standish Group. (2014). *The Standish Group report: Chaos.*

The Water Environment Federation. (2007). *Automation of wastewater treatment facilities – 3rd edition. ISBN: 978007149370.*

The Water Environment Federation. (2010). *Design of municipal wastewater treatment plants – 5th edition. ISBN: 9780071663588.*

Tohidi, M. (2011). *The role of risk management in IT systems organisations. Procedia Computer Science. 3. Pages 881-887.*

Trochim, M.K.W. (2006). *Deductive and inductive thinking. www.socialresearchmethods.net/kb/dedind.php.*

Uçaktüçrk, A. & Villard, M. (2013). *The effects of management information and ERP systems on strategic knowledge management and decision-making. Procedia Social and Behavioral Science. 99. Pages 1035-1043.*

United Nations. (2008). *Millennium development goals.*

Urban Land Institute. (2011). *Infrastructure 2011: A strategic priority.*

van der Voet, J. (2014). *The effectiveness and specificity of change management in a public organisation - Transformational leadership and a bureaucratic organisational structure. European Management Journal. Issue 32. Pages 373 – 382.*

van Grembergen, W. (2002). *Introduction to the minitrack: IT governance and its mechanisms. In proceedings of the 35th Hawaii international conference on systems science (HICCS).*

van Grembergen, W., de Haes, S. & Guldenstops, E. (2004). *Structures, processes and relational mechanisms for IT governance. In: Van Grembergen, W. Strategies for information technology governance. Hersey, P.A.: Idea Group Publishing. Pages 1-36.*

van Niekerk, B. & Maharaj, M.S. (2011). *The information warfare life cycle model, SA Journal of Information Management 13(1). Pages 187-194.*

Verhoef, C. (2007). *Quantifying the effects of IT-governance rules. Science of Computer Programming. 67. Pages 247-277.*

von Petersdorff, H.A. (2013). *Identifying and quantifying maintenance Improvement opportunities in physical asset management. Department of industrial engineering – University of Stellenbosch. http://scholar.sun.ac.za/handle/10019.1/85699.*

von Solms, R. & von Solms, S.H. (2006). *Information security governance: Due care. Computers & Security. 25. Pages 494-497.*

von Solms, R. & von Solms, S.H. (2006). *Information security governance: A mode based on the direct-control cycle. Computers & Security. 25. Pages 408-412.*

Wang, W. & Shuo, L. (2013). *Cyber security in the smart grid: Survey and challenges. Computer networks. 57. Pages 1344-1371.*

Webb, J., Ahmad, A., Maynard, S.B. & Shanks, G. (2014). *A situation awareness model for information security risk management. Computers & Security. 44. Pages 1-15.*

Weill, P. & Ross, J.W. (2004). *IT governance – How top performers manage IT decision rights for superior results. Boston: Harvard Business School Press.*

Wendler, R. (2012). *The maturity of maturity model research: A systematic mapping study. Information and Software Technology. 54. Pages 1317-1339.*

Woodhouse, J. (2010). *Asset management: The way forward. Whole-life management of physical assets. Pages 209-221. ISBN: 798-0-7277-3653-6.*

World Bank. (2006). *The challenges of reducing non-revenue water in developing countries.*

World Economic Forum. (2013). *Strategic infrastructure: Steps to prepare and accelerate public-private partnerships. Geneva.*

World Economic Forum. (2014). *Strategic infrastructure: Steps to operate and maintain infrastructure efficiently and effectively.*

World Economic Forum. (2015). *Industrial internet of things: Unleashing the potential of connected products and services.*

World Federation of Exchanges. *(2013). 2012 WIFE market highlights. January, 2013.*

World Health Organisation & United Nations Children's Fund, (2009). *Diarrhoea: Why children are still dying and what can be done. Geneva.*

Yin, K.R. (2003). *Case study research: Design and methods. Beverly Hills CA: Sage Publications.*

Zachman, J.A. (1987). *A framework for information systems architecture. IBM systems journal. 26 (3). Page 276-292.*

Zachman, J.A. (2003). *The Zachman framework for enterprise architecture: Primer for enterprise engineering and manufacturing.*

Zandi, F. & Tavana, M. (2012). *A fuzzy group multi-criteria enterprise architecture framework selection model. Expert Systems with Application. 39. Pages 1165-1173.*

Zhang, Z. & Guo, G. (2014). *An approach to group decision making with heterogeneous incomplete uncertain preference relations. Computers & Industrial Engineering. 71. Pages 27-36. Dilian University of Technology.*

Zhiwei, Y & Zhongyuamn, J. (2012). *A survey on the evolution of risk evaluation for information systems security. Energy Procedia. 17. Pages 1288-1294.*

Annexure A - Rand Water Way Detail Characteristics

The purpose of this annexure is to describe additional characteristics of the Rand Water Way, as defined in chapter 5. It provides a more detailed description of the characteristics and nature of the transition roadmap, as well as the phases and stages of the roadmap.

A.1. Transition Roadmap Characteristics

There are key characteristics of the transition roadmap that contribute to its appropriateness for implementing digital governance in a large and complex asset intensive organisation. These are: 1) time and vision-based incremental value delivery; 2) quick wins with acceptable residual risk; 3) evolving roles of participating digital functions; 4) flexible and adaptive management; and 5) the continuous nature of the stages. Each of these key characteristics will be described in more detail.

The transition roadmap is ***time and vision-based***. A vision is defined for the roadmap to direct the overall transition and to motivate the leadership to accept the risk and embark on the journey to achieve the expected value *(Goss, Pascale & Athos, 1998; Martin, 1998; Augustine, 1998; East, 2011).* It represents the target state or desired level of maturity based on the overall philosophy and underling principles of the Rand Water Way *(Wendler, 2012; Becker, Knackstedt & Pöppelbuß, 2009).* The vision and the roadmap leading to the vision: 1) are defined and agreed by the stakeholders within the organisation; 2) are aligned to the organisation's strategic goals; and 3) address the real pain points of the organisation (*Kotter, 1995 & 1998; IT Governance Institute, 2012*). It therefore has legitimacy, in that it is credible, plausible and persuasive (*McDowall, 2012).* The roadmap defines a longer term transitional journey to implement enterprise-wide asset information management and digital governance in a large and complex organisation, rather than a once-off event *(Ross, 2004).* Such a journey is difficult, expensive, risky, long and without any short cuts (*Fonstad & Robertson, 2004; Ross. J, 2004*). The value will increase steadily and gradually through various incremental enhancements that are implemented as part of an evolutionary path to achieve the vision, desirable maturity or target state *(Becker,* Knackstedt & Pöppelbuß, *2009; Georghiou & Keenan, 2006).* The time and effort required to complete the initial "Building trust" related stages of the roadmap (e.g. Deliver on IT; Education and awareness; and Collaborate) depend on: 1) the reputation, credibility and legitimacy of the digital function proposing the change;

and 2) the willingness of other digital functions to collaborate and cooperate with that digital function. The least amount of time will probably be required to complete the middle "Efficiency" related stages (e.g. Support services; Exploit convergence; and Integrate), because these stages deliver the majority of the direct and visible benefits to the digital functions participating in this journey. However, it will depend on the available opportunities and needs, because these stages are primarily opportunistic and are based on business needs and priorities (e.g. convergence in telecommunications; system integration needs). The "Formalisation" related stages (e.g. Architecture; Strategy; Governance; and Controls) will probably require the most amount of time, since these stages require a formal longer term compliance commitment from all stakeholders. This attribute of the roadmap will be described in more detail as part of the "evolving roles of participating digital functions" characteristic.

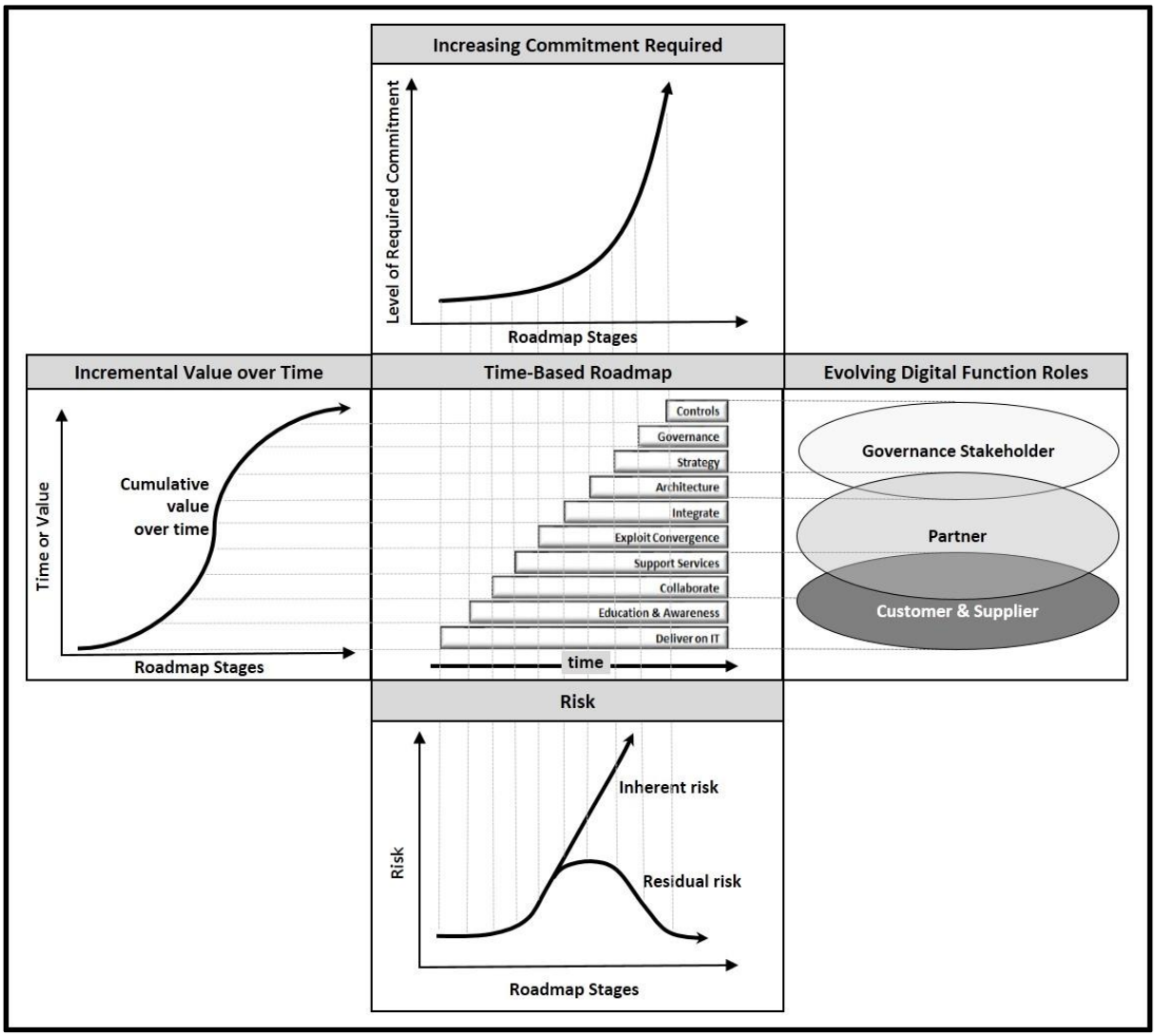


Figure A-1 Transition Roadmap Characteristics

The transition roadmap includes ***"quick wins" with an acceptable level of residual risk.*** The transition roadmap, like all other change initiatives, has some inherent risk to the current operations or the individuals impacted by the transition *(Fonstad & Robertson, 2004; Goss, Pascale & Athos, 1998).* These risks must be acceptable to the stakeholders if the desired value is to be realised *(Kotter, 1998; Johnson, 2010).* Even though there are no short cuts on this journey, the roadmap includes interim results-based improvements with clear benefits to the organisation, in addition to the longer-term activity-based improvements (e.g. formalised digital governance) *(Schaffer & Thomson, 1998).* The benefits of the change are made visible and evident at various milestones during the implementation (e.g. quick wins, short-term opportunities, "low-hanging fruit") *(Ross, 2004; Fonstad & Robertson, 2004)*. This is done in order to keep the momentum of the change initiative *(Kotter, 2012; Kotter & Schlesinger, 2008).* These quick wins pose a risk to the organisation, because the associated operational process controls might not have been formalised and implemented at that point in the roadmap. An example of such a scenario is the integration of the IT and control systems in the absence of an agreed enterprise-wide digital architecture and relevant operational process controls, required to mitigate the risk to the overall landscape (e.g. digital configuration management). In this example the residual risk for the proposed quick wins approach is kept at an acceptable level by: 1) basing the system integration on the existing IT architecture and the control system designs; 2) implementing the minimum critical preventative security controls (e.g. malicious software protection); and 3) relying temporarily on the existing operational controls practised by the individual digital functions. The residual risk is further reduced by limiting the integration to low risk solutions (e.g. integrating control system data for reporting purposes). Additional system integration that poses a higher risk to the digital landscape (e.g. integrating control system data to IT systems for further processing) will only be performed once the relevant essential operational process controls have been formalised and implemented. The proposed quick win approach ensures that: 1) the benefits of the change are visible as soon as possible; 2) the necessary buy-in and commitment is obtained from the control system functions; and 3) the momentum of the transition journey is maintained, without exposing the infrastructure installations, business and digital landscape to an unacceptable level of risk. The alternative zero-risk approach would be firstly to define, approve and implement all the required formalised operational process controls to mitigate all potential risks, before integrating the IT and control systems. This zero-risk approach will only make the benefits visible at the end of the longer term transition roadmap. It will require all the digital functions to commit to, and spend resources and time on, developing, implementing and complying with

enterprise-wide operational process controls, without any visible evidence that the change will deliver the expected benefits. The zero-risk approach is not suitable for a large and complex asset intensive organisation with segregated digital functions or business units.

The ***role of the participating control system functions changes over time*** as progress is made along the transition journey. To illustrate this characteristic, it is assumed that: 1) the control system and IT functions are segregated; and 2) the corporate IT function is proposing and leading the transition journey. During the initial stages of the roadmap (e.g. Deliver on IT), the role of the control system function is that of a customer of the IT function *(Nfuka & Rusu, 2010; The Standish Group, 2014).* An additional role is added to the control system function during the efficiency related stages of the roadmap (e.g. Collaborate, Exploit convergence, Integrate), namely that of a business partner. All digital functions have a shared responsibility towards one another for the success of these roadmap stages in order to achieve the expected efficiency improvements *(Kotter & Schlesinger, 2008; Flores, Antonsen. & Ekstedt, 2014).* Participation, involvement and collaboration are required from all digital functions for these stages to be successful *(Prasad, Green & Heales, 2012; Flores, Antonsen. & Ekstedt, 2014).* However, it remains voluntary and the control system function still has the opportunity at this point to withdraw from this transition journey. A point of no return is reached during the latter stages of the efficiency related phases (e.g. digital consolidation). The voluntary involvement changes to formal commitment by the control system function *(Weill & Ross, 2004; Sambamurthy & Zmud, 1999).* When the formalisation related stages are reached (i.e. Architecture, Strategy, Governance, Controls), a significant change takes place in the role of the control system function. The required level of commitment increases exponentially. The deliverables of these phases (e.g. architecture, standards, policies, strategy) are approved at an executive or board level. Compliance to these deliverables is compulsory and independent assurance of such compliance becomes applicable *(Webb, Ahmad, Maynard & Shanks, 2014; Shamala, Ahmad & Yusoff, 2013).* This previously autonomous or isolated IT customer is now accountable to the established digital governance structures, such as the digital steering committee *(Kooper, Maes & Lindgreen, 2011; van Grembergen, de Haes & Guldenstops, 2004).* The management of the control system function must come to understand that it will be acting under new constraints to achieve new purposes, and that its goals must be aligned to those of the digital group as a whole *(de Vreede & Briggs, 2005).* This change in the role of the control system function from IT customer, to voluntary business partner, and finally to committed and accountable digital governance stakeholder, can have a devastating effect on

the success of the transition journey, if not recognised and taken into account by the organisational change management efforts of the transition management approach *(Kotter, 1995).*

The transition roadmap is ***consistent with reflexive, adaptive management*** because the longer term transition journey is not always a simple straight line *(McDowall, 2012).* There is adequate flexibility within the roadmap to make the necessary "course corrections", whilst still retaining the overall vision *(Anderson & Anderson, 2001).* This flexibility is built into the roadmap in order to: 1) cater for some degree of uncertainty about the future state; and 2) be responsive to new opportunities, lessons learnt, and changes in the environment that might take place during the execution of the roadmap *(McDowall, 2012).* The roadmap also avoids the notion of a "one size fits all" framework and a "cookbook recipe for success" *(Verhoef, 2007; Lunardi, Becker, Maçada & Dolci, 2014).* It includes adequate flexibility for it to be contextualised based on the characteristics of an organisation, in order for it to be useful to that organisation *(East, 2011; Pilling, 2010; McDowall, 2012).* This includes: 1) the time allocated to the trust building related stages of the roadmap based on the current reputation and legitimacy of the digital function proposing or leading the change; 2) the current level of digital governance maturity of the organisation; and 3) the identification and sequencing of the quick wins, ongoing activities and projects to be executed within the stages of the roadmap, based on the organisation's risk appetite and urgency for change *(Kotter & Schlesinger, 2008;Wendler, 2012).* The adaptability of the transition roadmap ensures an implementation approach that: 1) is appropriate for the organisation; and 2) has a higher probability of value delivery and achieving the stated vision.

The ***stages of the transition roadmap are continuous in nature.*** The stages are not purely sequential or discrete once-off events, as per a typical maturity model definition (i.e. "step ladder" approach) *(Wendler, 2012).* Each stage provides the prerequisite foundation for the next stage to start and to be successful. Each stage is also a continuous work stream, journey, or evolutionary path with interdependencies between its activities and/or other stages. It includes a gradual improvement in maturity via various incremental enhancements over time *(Becker, Knackstedt & Pöppelbuß, 2009; Kaplan & Norton, 2001).* This ensures that the complex problem of implementing enterprise asset information management, enterprise architecture, and the governance of asset information and digital technology in a large, complex heterogeneous asset intensive organisation is addressed, by breaking the problem up into smaller individual problems and opportunities *(Kluth, Jäger, Schatz & Baurenhansl, 2014).*

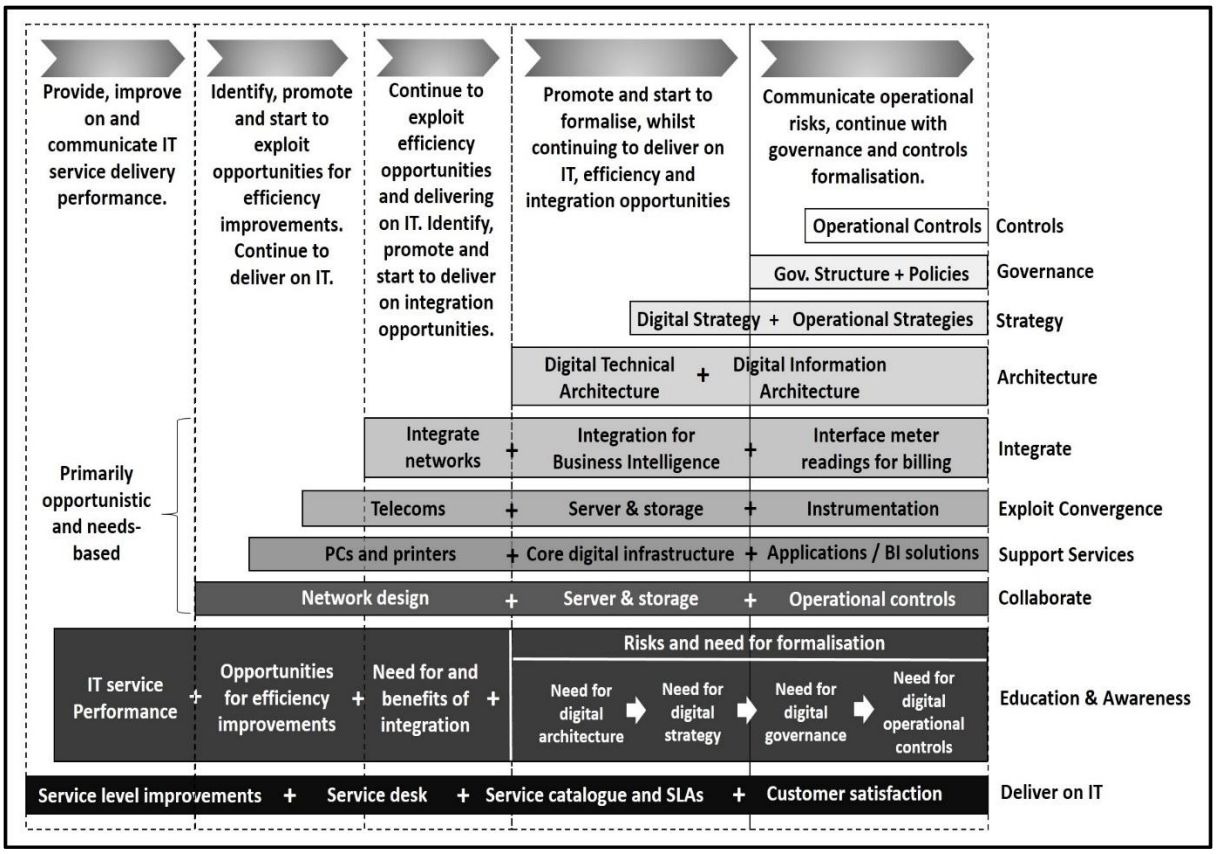


Figure A-2 Continuous Nature of Transition Roadmap Stages

The education and awareness stage is used to illustrate this characteristic. Formal communication is continuous throughout the duration of the transition journey. It is not a once-off event only to make stakeholders aware of the vision. The content and purpose of the communication interventions change over time. For example, the initial communication may focus on IT service delivery, in order to build trust in the capability of the IT function to lead the transition. In addition, the need and opportunity for efficiency improvements (e.g. convergence of IT and telemetry networks) are communicated before the convergence in network technology is exploited during the Exploit Convergence stage. The same applies to: 1) the benefits and need for IT and control system integration and the integration stage; and 2) the risks associated with the lack of an enterprise architecture, governance mechanisms and operational process controls and the formalisation related stages. The same continuous nature also applies to other stages of the transition roadmap. The improvement activities or projects, to be performed as part of these stages, are sequenced and prioritised based on: 1) opportunities and needs of control system and business functions (e.g. collaboration projects; providing support services; integrating IT and control systems); and 2) risk and urgency (e.g. exploit convergence in technology for lower risk solutions first; implement the most critical operational process controls first).

A.2. Transition Roadmap Phases and Stages

Each of the phases of the transition roadmap will be defined in more detail in terms of its purpose, its stages and the benefits of completing this phase as part of the journey.

Phase 1 - Cement Foundation

The purpose of this phase is to establish and cement the foundation required for the collaboration between the digital functions during the rest of the transition journey. The emphasis is on: 1) cultivating trust in the capability and intention of the digital function that proposes or leads the transition journey; 2) improving the legitimacy of the digital function that proposes or leads the transition journey; and 3) informing and educating the digital functions of the organisation regarding various aspects of the transition and the phases of the roadmap. This phase includes the following two stages:

Stage	Description
Deliver on IT	Delivering on IT consists of delivering good quality services by the IT function proposing and leading the transition. This assumes that the corporate IT function is the digital function proposing and leading the transition. The IT customers include the control system functions. The maturity of IT service delivery may increase over time, including the establishment of an IT service desk, IT service catalogue, IT service level agreement, IT customer satisfaction measurements, and IT service quality measurements and reporting. It is important that the quality and maturity of IT service delivery is maintained during the life of the transition, in order to maintain the foundation and legitimacy of the IT function to lead the transition.
Education & awareness	The formal education, communication and explicit knowledge transfer interventions that focus on the required digital subjects and all the digital functions of the organisation. The required subjects include opportunities to improve efficiencies, digital strategy, digital governance, the need to change, the vision or "big picture", and the transition roadmap to achieve the vision. It includes practical and related digital subjects in support of the transition, such as digital enterprise-architecture, information management and security related risks and threats. The topics and formality of the education and awareness may change over time. It should relate to the current or next stage of the roadmap to be performed. The education and awareness efforts are ongoing and may have to be repeated due to changes in management and / or members of the digital functions.

Table A-1 Cement Foundation Phase Stages

The completion of the stages of this phase will ensure that the following outcomes are reached:

Outcome	Description
Established legitimacy, credibility, reputation and integrity.	The legitimacy, credibility, reputation and integrity of the digital function leading the change (i.e. corporate IT function) is established by illustrating the quality and capabilities of the IT function *(Nfuka & Rusu, 2010; The Standish Group, 2014; Kotter, 2012).*
Increased willingness to participate and collaborate.	The willingness of the other digital functions to participate in and collaborate with the leading digital function during the rest of the change journey is increased *(Kotter, 2012; Duck, 1998).*
A sense of urgency created.	A sense of urgency is created for the change, by helping others to see the need to change, communicating the vision for buy-in, improving transparency and reducing misunderstanding in terms of the vision and the roadmap *(Kotter & Schlesinger, 2008; Ross, 2004; Strebel, 1998).*
Improved stakeholder knowledge, contribution and decision making capability.	All the stakeholders, including the other digital functions, can make a meaningful contribution to the joint digital future of the organisation and make informed decisions based on relevant and up to date knowledge. This includes knowledge of the "big picture", the potential benefits of the change and the risks facing the organisation *(Ahmad, Hadgkiss & Ruighaver, 2012; Shedden, Scheepers, Smith & Atif, 2011; Colwill, 2009; Shedden, Ruighaver & Ahmad, 2010).*
Legitimate vision agreed.	The agreed vision will have legitimacy in terms of credibility, plausibility, and appropriateness. This is achieved by ensuring that informed and knowledgeable stakeholders, including all the digital functions, participate in shaping the shared digital vision *(McDowall, 2012; Kotter, 2012).*
Improved two-way communication in place.	One of the primary causes of resistance to change, namely the lack of repeated two-way communications, is prevented, or overcome *(Kotter & Schlesinger, 2008; Othman, Chan & Foo, 2011; Goss, Pascale & Athos, 1998).*

Table A-2 Cement Foundation Phase Outcomes

Phase 2 - Joint Endeavours

The purpose of this phase is to further cultivate trust between the digital functions and to start to achieve efficiencies. This is achieved by jointly addressing common objectives, or problems, and providing shared, or common, digital services to the other digital functions. Trust, in the context of this stage, refers to trust in the capability and intention of the digital function leading the transition

This phase includes the following two stages:

Stage	Description
Collaborate	Collaboration between digital functions, in order to achieve common objectives, resolve common problems, share scarce digital expertise, and assist other digital functions, where needed and possible. This includes smaller improvements and large digital projects (e.g. converged network design for large scale remote SCADA systems). These collaboration initiatives are voluntary and depends on the available opportunities and needs.
Support services	Providing IT support services to control system functions, or other IT functions, where needed or requested, with the emphasis on converged digital infrastructure or essential operational process controls (e.g. maintenance of SCADA servers; malicious software protection). These services are voluntary and require a willing customer. It depends on the available opportunities and needs. Low risk services are initially offered (e.g. PC maintenance) and may evolve to more advanced and higher risk services (e.g. SCADA server maintenance).

Table A-3 Joint Endeavours Phase Stages

The completion of the stages of this phase will ensure that the following outcomes are reached:

Outcome	Description
Improved utilisation of scarce digital skills and resources.	Scarce skills and converged digital technology related expertise are shared and utilised in a cost effective manner across the digital landscape and functions, especially where cross skilling is either not feasible or not a high priority *(Flores, Antonsen & Ekstedt, 2014; Jaatun, Røstum, Peterson & Ugarelli, 2014).*
Improved knowledge transfer and skills development.	The formal education and awareness interventions are supplemented by informal cross-training of digital staff members from the different digital functions and the transferring of information and tacit knowledge. This includes knowledge related to digital initiatives, best practices, system interoperability related risk, security threats, as well as the real way that the organisation works and the real pain points or weaknesses of the organisation that the change should address *(Flores, Antonsen & Ekstedt, 2014; Anwar & Mahmood, 2014; Ahmad, Hadgkiss & Ruighaver, 2012; Goss, Pascale & Athos, 1998).*
Digital function collaboration and cooperation.	Digital functions start working together across organisational boundaries towards a common goal. Expertise from all stakeholders is utilised. Staff from the various digital functions participate by jointly planning, defining or designing and implementing improvements or solutions to problems *(Hadaya & Cassive, 2012; Lloyd, 2012; Soloman, 2010).*

Table A-4 Joint Endeavours Phase Outcomes

Phase 3 - Digital Consolidation

The purpose of this phase is to further achieve efficiencies and to start to deliver fused and harmonised asset data from across the digital landscape. This is achieved by consolidating the digital landscape by exploiting the convergence in digital technology and by integrating the digital technology, systems and asset information. This phase includes the following two stages:

Stage	Description
Exploit convergence	Exploit the convergence in digital technology between IT and control systems (e.g. unified communications / convergence in communication network technologies, SCADA server technology), where feasible and agreed. This is done in order to consolidate and simplify the digital technology landscape. It should be achieved without increasing the risk to the core operations and the infrastructure installations to an unacceptable level.
Integrate	Integrate IT and control systems, including the asset information and underlying digital infrastructure. This includes the control and IT networks, as well as the actual IT and control systems. Integration of asset data is first limited to reporting purposes (e.g. SCADA data integrated to the IT data warehouse) and later on for further processing (e.g. master data for customer billing purposes). This should be achieved without increasing the risk to the core operations and the infrastructure installations to an unacceptable level.

Table A-5 Digital Consolidation Phase Stages

The completion of the stages of this phase will ensure that the following outcomes are reached:

Outcome	Description
Optimal digital landscape.	The digital technology landscape is optimised and cost effective. The ability and probability of successful integration of digital systems and asset data is improved, via an enterprise-wide converged and integrated digital infrastructure landscape *(ISO, 2014; Soloman, 2010; The Water Environment Federation, 2007 & 2010).*
Change momentum maintained.	The momentum of the overall change initiative is maintained and the platform for further change is established. This is achieved by illustrating the benefits of the change as soon as possible in the transition roadmap, making it evident to the digital functions within the organisation, and exploiting short to medium term opportunities *(Kotter, 1995 & 1998; Schaffer & Thomson, 1998; Augustine, 1998).*
Integrated asset data and underlying digital technology.	Asset data becomes useful for asset management, in that it is shared timeously with other systems and users for either operational transactional processing purposes and/or for asset management decision making purposes *(ISO, 2014; Lloyd, 2012; Fernández-de-Alba, Fuentes-Fernández & Pavón, 2013; Chang, Kauffman & Kwon, 2014).*

Table A-6 Digital Consolidation Phase Outcomes

Phase 4 - Digital Future

The purpose of this phase is to define the digital future for the enterprise, including all the digital functions. It will start to reduce the operational risk, obtain formal longer-term commitment from stakeholders and institutionalise the change. This is achieved by formalising and agreeing on the relevant digital strategy(ies) and an enterprise architecture for the entire digital landscape. All digital functions should comply with the co-created and approved enterprise architecture and digital strategy(ies). This phase includes the following two stages:

Stage	Description
Architecture	Define, agree, implement and comply with an enterprise architecture (i.e. business, information, technology) and related digital standards. It includes the to-be architecture and the security architecture. The enterprise architecture applies to all digital functions and solutions of the organisation. This stage includes the definition of an enterprise information management framework and the application of the information management activities to all asset data across the digital landscape.
Strategy	Define and formalise a common digital strategy(ies) and strategic plans for the organisation and / or align the various digital strategies of the organisation, where needed and feasible (e.g. how to address the convergence in digital technology).

Table A-7 Directed Future Phase Stages

The completion of the stages of this phase will ensure that the following outcomes are reached:

Outcome	Description
Reduced interoperability risk.	The digital technology interoperability and incompatibility risk is adequately mitigated. The digital technology, system and information landscape is, and will continue to be, integrated and enable asset data to be timeously shared or exchanged with other systems and users *(The Open Group, 2009; Iyamu, 2011; Kang, Lee, Choi & Kim, 2010; von Petersdorff, 2013).*
Asset information managed as strategic enterprise resource.	A consistent, harmonised and quality set of data is delivered timeously and exploited for asset management decisions. This is achieved by: 1) managing asset information as a strategic resource at an enterprise level; 2) and applying information management activities to all asset information, independent of its origin *(Fernández-de-Alba, Fuentes-Fernández & Pavón, 2013; Kang, Lee, Choi & Kim, 2010; Lehman & Heagy, 2014; Uçaktüçrk & Villard, 2013; Dhami & Thomson, 2012).*

Outcome	Description
Reduced digital technology size and complexity related risk.	The risks related to a large, complex, sophisticated, heterogeneous digital landscape of an asset intensive organisation are reduced to an acceptable level. This includes the implementation of digital technology changes within such an environment *(ISO, 2014; King & Knight, 2003; Hammoudech & Newman, 2013; Rice & Almajali, 2014; Kluth, Jäger, Schatz & Baurenhansl, 2014).*
Reduced big data related risk.	The information management and security risks related to "big data" (e.g. volume, variety, velocity and value) are reduced to an acceptable level. This allows quality data to be produced for asset management decision making *(Woodhouse, 2010; Kwon, Lee & Shin, 2014; Chen & Zhang, 2014; Burns, 2010; von Petersdorff, 2013; Edwards, 2010; Chang, Kauffman & Kwon 2014).*
Agreed digital future.	The future of the digital landscape is defined and agreed via the enterprise architecture and digital strategy(ies). It is aligned with the corporate strategy, the asset management strategy and strategies of the digital functions and/or business units of the organisation *(Kaplan & Norton, 2001; Bowen, Chung & Rohde, 2007; Leill-Cock, Graham & Hill, 2009; Kang, Lee & Kim, 2010; Šaša & Krisper, 2011; Iyamu, 2011).*
Reduced digital information security risk.	The digital security risk for the overall digital landscape is partially addressed via an agreed enterprise information security architecture and information security activities applied to all asset data across the digital landscape *(Shariati, Bahman & Shams, 2011; Rice. & Almajali, 2014; Anwar & Mahmood, 2014; Wang & Shuo, 2013; Pulkkinen, Naumenko & Luostarinen, 2007).*
Formalised commitment received from all stakeholders.	Formalised commitment and buy-in, rather than only voluntary involvement, is obtained for the digital future of the organisation from all stakeholders, including executive management, the board of the organisation and all digital functions *(Spears, Barki & Barton, 2013; Kotter, 1998; Tohidi, 2011; Prasad, Heales & Green, 2010).*
Institutionalised or embedded change in terms of future.	The change is institutionalised, or embedded, into the organisation's digital future via the enterprise architecture, standards and strategy(ies) *(Spears, Barki & Barton, 2013; van der Voet, 2014; Kotter, 1998).*

Table A-8 Directed Future Phase Outcomes

Phase 5 - Governed Landscape

The purpose of this phase is to further obtain formal commitment from stakeholders, institutionalise the change and reduce the operational risk to an acceptable level for the entire integrated digital landscape. This is achieved by focusing on the governance mechanisms and operational process controls for the entire digital landscape. All digital functions must comply with these mechanisms and controls.

This phase includes the following two stages:

Stage	Description
Governance	Define, formalise, agree on and implement the essential digital governance mechanisms at an enterprise level. Ensure that important digital governance mechanisms are identified, agreed to and implemented by individual digital functions or business units. The resulting digital governance framework includes the digital governance structure, policies, decision making authorities, and processes.
Controls	Define, formalise, agree and implement the "essential" digital internal / management / operational process controls at an enterprise level and on a centralised basis. Ensure the implementation of the "important" operational process controls by individual digital functions / business units on a federated basis. Monitor compliance of these "important" controls to relevant enterprise-wide rules or directives (e.g. digital policies).

Table A-9 Governed Landscape Phase Stages

The completion of the stages of this phase will ensure that the following outcomes are reached:

Outcome	Description
Ability to achieve longer term asset management objectives.	The organisation will: 1) achieve its ***longer term*** asset management related goals; 2) deliver value through effective governance and management of digital technology and asset information; 3) encourage desirable behaviour in the use of digital technology by all digital functions; and 4) create optimal and sustainable value from digital technology, by maintaining a balance between realising benefits, or value delivery, and optimising risk levels *(Verhoef, 2007; ISO, 2008; Weill & Ross, 2004).*
Mitigate residual operational digital risks.	Further mitigate those residual risks that were accepted during the transition journey, in order to illustrate the benefits of the change as soon as possible and to maintain the change initiative momentum *(Prasad, Heales & Green, 2010; Kluth, Jäger, Schatz & Baurenhansl, 2014; Benaroch, Chernobai & Goldstein, 2012; Gheorghe, 2010).*
Formalised longer term commitment and buy-in.	Obtained formalised commitment and buy-in from all stakeholders for the governance mechanisms and operational process controls of the organisation. This includes commitment from executive management, the board and all digital functions of the organisation *(Spears, Barki & Barton, 2013; Kotter, 1998; Tohidi, 2011; Prasad, Heales & Green, 2010).*
Institutionalised or embedded change in the way of working.	The change is institutionalised, or embedded, into the organisation's culture, way of thinking and way of working, via the digital governance mechanisms and internal operational process controls (e.g. information security management) (*Spears, Barki & Barton, 2013; Bowen, Chung & Rhode, 2007; Anwar & Mahmood, 2014; Wang & Shuo, 2013; Kotter, 1998).*

Table A-10 Governed Landscape Phase Outcomes

Annexure B - Rand Water Way Evaluation Details

The purpose of this annexure is to provide supplementary details of the evaluation of the Rand Water Way, as described in chapter 7. This includes the questionnaires used, the description of the similar participating organisations, as well as the detailed responses from the expert panel members.

B.1. Rand Water Evaluation

The following questionnaire was used for evaluating the Rand Water instantiation of the Rand Water Way:

Position of respondent	

		Rating				
	Please select the most appropriate response for each of the statements.	**1 - Strongly disagree**	**2 - Disagree**	**3 - Neutral**	**4 - Agree**	**5 - Strongly Agree**
Statements						
A	**Usefulness**					
A.1	**Problem relevance:** Are / were the statements below applicable to the Rand Water environment?					
A.1.1	**Technology and information related problems**					
1.1.1	**ICT landscape size and complexity:** The ICT landscape, including IT and OT systems, is large, complex and heterogeneous in nature.					
1.1.2	**ICT isolation and incompatibility:** OT systems are isolated and / or incompatible with IT systems and does not allow information to be exchanged between OT and IT systems.					
1.1.3	**Fast pace of ICT development:** ICT and the convergence between OT and IT are developing at a fast pace.					
1.1.4	**Diverse information source:** Information originates and is stored across the ICT landscape (OT and IT systems).					
1.1.5	**Inconsistent information management:** Information is not managed consistently and rigorously across the ICT (OT and IT systems) landscape (e.g. naming conventions, format, data quality, classification, ownership).					

Please select the most appropriate response for each of the statements.		Rating				
		1 - Strongly disagree	2 - Disagree	3 - Neutral	4 - Agree	5 - Strongly Agree
Statements						
1.1.6	**Big Data:** Information volume (e.g. storage size, number of data items / data granularity) and variety (e.g. format, medium) is high and increasing (e.g. asset condition assessments).					
A.1.2	**Process related problems**					
1.2.1	**Security threats:** Information security (e.g. availability, integrity, confidentiality) threats (e.g. malicious software, unauthorized access, natural disasters) pose a risk to the overall ICT landscape, especially in the case of an integrated ICT landscape.					
1.2.2	**Governance maturity inconsistency:** The maturity of ICT governance and operational controls differ between OT and IT system functions and / or solutions.					
1.2.3	**Compliance as end goal:** The primary purpose of ICT / IT governance is compliance to a standard, code or framework rather than a means to effectively mitigate associated operational risks.					
1.2.4	**Operational control inadequacy:** The operational process controls of the IT and/or OT systems do not provide adequate assurance that quality data will be made available timeously for decision making.					
1.2.5	**Lack of alignment:** There is no alignment between the OT and IT functions in terms of future direction, to-be / vision architecture and standards or common strategic goals.					
A.1.3	**People and organisational related problems**					
1.3.1	**Organisational structure:** The OT and IT functions report to different functional / organisational / business units of the organisation (organisational segregation).					
1.3.2	**Lack of trust:** There is a lack of trust in the IT function, by the OT functions, either in terms of capability (e.g. credibility, capacity, skills, track record) and / or intention (e.g. empire building), leading to a lack in legitimacy to lead this journey.					
1.3.3	**Resistance to change:** There is generally resistance to change by OT and / or IT functions, including this change initiative.					
1.3.4	**Lack of vision and/or urgency to change:** There is a lack of an agreed shared vision related to ICT governance and/or a sense of urgency to change.					
1.3.5	**Change forum / coalition:** There is a lack of a change forum or coalition that will market, support and/or drive this change (e.g. team, committees, etc.)					
1.3.6	**Lack of collaboration, involvement and sharing:** There is a lack of collaboration (e.g. joint projects), resource / skills / expertise sharing (e.g. support services), involvement in decision making and / or communication between IT and OT functions.					

Please select the most appropriate response for each of the statements.		Rating				
		1 - Strongly disagree	2 - Disagree	3 - Neutral	4 - Agree	5 - Strongly Agree
Statements						
A.2	**Problem resolution** Will the Rand Water approach resolve the challenges relevant to the Rand Water environment?					
A.2.1	**Technology and information problem resolution**					
2.1.1	**Complexity, size and pace of change:** It will address the complexity, size and fast pace of change and convergence of the ICT (OT & IT) landscape					
2.1.2	**Information exchange:** It will assist in enabling information to be exchanged between OT and IT systems in support of decision making, via integration and compatible technology.					
2.1.3	**Information fusion:** It will assist in ensuring that the required information from across the ICT landscape is fused or harmonised, where required, to provide an integrated set of information in support of business decision.					
2.1.4	**Data quality:** It will assist in ensuring that information has the required level of quality (e.g. completeness, correctness) to support effective decision making.					
A.2.2	**Process problem resolution**					
2.2.1	**Cyber security threats:** It will assist in ensuring that the ICT / cyber security (i.e. availability, integrity, confidentiality) threats and risks are adequately mitigated for the integrated ICT landscape, including the "weakest links".					
2.2.2	**Lack of operational controls:** It will adequately address the risk related to the lack of operational controls (e.g. change and configuration management), including the related common operational or strategic ICT risks.					
2.2.3	**Value delivery beyond compliance**: It will assist in ensuring that the governance mechanisms and operational process controls deliver value beyond compliance to a regulation, code, standard or framework (e.g. risk mitigation, real pain points).					
2.2.4	**Avoid over and under-regulation:** It will prevent the negative implications of over and under regulation of the ICT environment, namely inadequate risk reduction and / or inefficiency / productivity loss.					

Please select the most appropriate response for each of the statements.	Statements	Rating				
		1 - Strongly disagree	2 - Disagree	3 - Neutral	4 - Agree	5 - Strongly Agree
A.2.3	**People and organisational problem resolution**					
2.3.1	**Improve involvement and commitment:** It will ensure involvement and / or commitment from all internal stakeholders across the organisation to this change journey and related decision making.					
2.3.2	**Reduce resistance to change:** It will reduce and / or eliminate the resistance to this proposed change in the way of thinking about ICT governance within the organisation.					
2.3.3	**Improve trust:** It will improve the trust between the ICT functions in terms of capability and / or intention, and thereby the credibility and legitimacy of the IT function to propose and/or lead this change journey.					
2.3.4	**Improve collaboration and sharing**: It will improve the collaboration and communication between the ICT functions of the organisation, as well as the sharing of skills and expertise.					
2.3.5	**Shared vision and direction:** It will ensure a common, aligned and shared vision and future direction for the digital functions, especially related to ICT governance.					
2.3.6	**Sustainability of change:** It will ensure a sustainable change in the way of thinking about ICT governance across the organisation and ICT functions will continue to comply with the agreed governance mechanisms and operational controls ("make it stick"; embed the change).					
B	**Usability**					
B.1	**Simplicity and clarity**					
B.1.1	**Simple:** The philosophy and underlying principles of the approach are simple, logical and straightforward.					
B.1.2	**Understandable / clear:** It is clear and easily understandable, including the philosophy, principles, framework and the constituent parts of the approach.					
B.1.3	**Adequately described:** The approach, including its constituent parts, are adequately defined and described.					
B.2	**Compatibility and flexibility**					
B.2.1	**Compatible:** It is compatible with the organisation (e.g. organisational structure; governance structures, culture).					
B.2.2	**Adequate guidance:** Adequate guidance is provided in terms of the application and implementation of the Rand Water approach.					
B.2.3	**Flexible / adaptive:** It is flexible, generic and adaptable enough to be contextualized or tailored for the organisation, where needed.					

Please write down any remarks regarding the advantages, disadvantages, strengths and weaknesses of the Rand Water Way approach. Where possible, relate it to one or more of the statements and criteria listed above.

Advantages / strengths of the approach
Disadvantages / Shortcomings of the approach
General Remarks

The statements related to the perceived usefulness evaluation are stated in the past tense, because it is an evaluation of an instantiated artefact. The problem relevance section evaluates the situation as at the start of the transition journey, namely 2007. Terminology was used in the questionnaire that the Rand Water digital functions are familiar with, in order to ensure that the statements in the questionnaire are correctly interpreted (e.g. "Information and Communications Technology / ICT" instead of "Digital Technology"; "Operational Technology / OT" instead of "Control Systems"). In some cases the expert panel includes more than one person per position, due to the staff turnover and changes in the organisation during the transition period. The expert panel for the Rand Water evaluation includes representatives from Asset Management (i.e. Senior Manager Assets - SMA), Control System functions (i.e. Manager Automation up to 2014 - MA2014, Manager Automation from 2015 - MA2015, and Manager Scientific Services Information Management – MSSIM), and the IT function (i.e. Manager IT Applications - MITA, IT Security Officer - ITSO, Manager IT Infrastructure and Operations - MITI&O and Manager Enterprise Architecture - MEA). Interviews were held with the expert panel members and the responses were recorded using the questionnaires. A deeper understanding of the reasons for the responses were obtained from the expert panel members.

The detailed responses received from each of the expert panel members during the ***usefulness*** evaluation of the Rand Water Way at the base case, Rand Water, are as follows:

Criteria / Statements		Respondents							
		SMA	MA2014	MA2015	MSSIM	MITA	ITSO	MITI&O	MEA
A	**Usefulness**	**4**	**4**	**4**	**4**	**4**	**4**	**5**	**5**
A.1	**Problem relevance**	**3**	**4**	**-**	**4**	**4**	**4**	**5**	**4**
A.1.1	**Technology and information problems**	**3**	**4**	**-**	**4**	**4**	**4**	**5**	**4**
1.1.1	Digital technology size and complexity	4	4	-	5	4	3	5	5
1.1.2	Digital isolation and incompatibility	2	2	-	2	4	4	4	4
1.1.3	Fast pace of digital technology development	2	2	-	5	4	4	4	4
1.1.4	Diverse asset information sources	4	4	-	5	4	4	5	4
1.1.5	Inconsistent asset information management	4	4	-	4	4	3	5	4
1.1.6	Big data (volume, variety)	4	5	-	4	4	4	5	4
A.1.2	**Process problems**	**4**	**4**	**-**	**4**	**4**	**4**	**4**	**5**
1.2.1	Security threats	4	5	-	5	4	4	4	5
1.2.2	Governance maturity inconsistency	5	4	-	5	4	4	5	5
1.2.3	Compliance as end goal	2	2	-	2	4	4	5	5
1.2.4	Operational control inadequacy	4	4	-	3	4	2	4	4
1.2.5	Lack of alignment	4	4	-	4	5	4	4	4
A.1.3	**People and organisational problems**	**3**	**3**	**-**	**3**	**4**	**4**	**5**	**5**
1.3.1	Organisational structure	5	5	-	4	4	5	5	5
1.3.2	Lack of trust (between digital functions)	3	4	-	1	4	3	4	4
1.3.3	Resistance to change	4	2	-	2	4	4	4	4
1.3.4	Lack of vision and/or urgency to change	2	4	-	2	4	4	5	4
1.3.5	Lack of change forum / coalition	2	3	-	4	5	4	5	5
1.3.6	Lack of collaboration and sharing	4	2	-	4	4	4	4	5
A.2	**Problem resolution**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**5**
A.2.1	**Technology and information problem resolution**	**5**	**4**	**4**	**4**	**4**	**4**	**4**	**4**
2.1.1	Complexity, size and pace of change	5	4	4	4	4	4	3	5
2.1.2	Asset information exchange	4	4	4	4	4	5	5	4
2.1.3	Asset information fusion	5	3	4	5	4	4	3	4
2.1.4	Asset data quality	4	4	4	4	5	4	3	4
A.2.2	**Process problem resolution**	**4**	**4**	**4**	**4**	**4**	**5**	**4**	**4**
2.2.1	Cyber security threats	5	4	4	4	4	5	5	4
2.2.2	Lack of operational controls	4	3	4	4	4	4	5	4
2.2.3	Value delivery beyond compliance	4	-	-	4	4	5	3	4
2.2.4	Avoid over and under-regulation	3	-	3	5	4	4	4	5
A.2.3	**People and organisational problem resolution**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**5**
2.3.1	Improve involvement and commitment	5	4	4	4	4	4	4	5
2.3.2	Reduce resistance to change	3	4	4	4	4	4	4	5
2.3.3	Improve trust (between digital functions)	4	5	4	4	4	4	4	5
2.3.4	Improve collaboration and sharing	4	3	4	4	5	5	4	5

Criteria / Statements	Respondents							
	SMA	MA2014	MA2015	MSSIM	MITA	ITSO	MITI&O	MEA
2.3.5 Shared vision and direction	4	4	4	4	5	5	4	5
2.3.6 Sustainability of change	5	3	4	4	4	4	4	5

Table B-1 Rand Water Usefulness Evaluation Responses

The following are the common phrases extracted from the remarks made by the expert panel regarding the perceived usefulness of the Rand Water Way:

Remark extracts / Common phrases	Respondents							
	SMA	MA2014	MA2015	MSSIM	MITA	ITSO	MITI&O	MEA
Advantages and strengths								
IT and OT system integration is beneficial.	x			x	x			x
Boundary between IT and control systems is grey.	x				x			x
ICT landscape is large and complex.	x	x		x	x		x	x
Control systems are isolated from IT systems.					x			x
Data in control systems is required for asset decision making.	x	x		x	x			x
Asset data is stored in diverse sources.	x				x			x
Asset data is integrated / harmonised.	x				x			x
OT can be integrated into IT systems.		x		x	x			
IT and IT systems are incorporated into the enterprise architecture.				x	x			x
Common asset information management is required.	x				x			x
Well balanced governance approach.	x			x				x
Information security is addressed.		x			x		x	
Governance and operational controls are beneficial.			x	x		x	x	
Operational controls not consistently applied.					x			x
IT and control systems functions involved.		x		x		x		
Formal executive commitment obtained.					x	x	x	x
ICT functions must work together.	x					x		x
Co-operation is in place.		x		x			x	
Agreed common ICT roadmap is key.		x		x		x		x
The change is sustainable.				x	x			x
Alignment between ICT functions is achieved.	x				x			x
Disadvantages and shortcomings								
System integration increases the security risk.		x					x	
ICT incompatibility is not a major risk.		x		x				
Might be considered as “red tape” at “grass roots”.		x	x				x	

Remark extracts / Common phrases	Respondents							
	SMA	MA2014	MA2015	MSSIM	MITA	ITSO	MITI&O	MEA
Role of ICT steering committee not clear.				x	x			x
OT data quality might not be assured.		x					x	
Change not adequately enforced via performance management.			x					x
Difference in ICT function mind set remains a problem.		x					x	
Lack of overall accountability for success of the approach.				x				x
Implementation is difficult, takes long.						x	x	
Difference in ICT function skills and capacity remain a problem.		x					x	
Different reporting lines and priorities remain a problem.						x	x	x

Table B-2 Rand Water Usefulness Remarks Extract

The common phrases relate to both the problem relevance and problem resolution sections of the questionnaire. It could either illustrate a positive (i.e. advantages or strengths) or negative (i.e. disadvantages or shortcomings) opinion regarding the perceived usefulness and usability of the Rand Water Way. The phrases were used as the basis for constructing the generalised statements of the expert panel members regarding the usefulness and usability of the Rand Water Way, as described in chapter 7. It also provided insight into: 1) the reasons for the quantitative responses of the expert panel members; and 2) the difference in the responses received from the different functions of Rand Water (i.e. asset management, control system functions and the IT function) and the organisations from different industries and sectors.

The detailed responses received from the expert panel members during the ***usability*** evaluation of the Rand Water Way at the base case, Rand Water, is as follows:

Criteria / Statements		Respondents							
		SMA	MA2014	MA2015	MSSIM	MITA	ITSO	MITI&O	MEA
B	**Usability**	**3**	**3**	**4**	**4**	**4**	**4**	**3**	**5**
B.1	**Simplicity and clarity**	**3**	**2**	**4**	**4**	**4**	**4**	**2**	**5**
B.1.1	Simple	3	2	4	4	4	3	3	5
B.1.2	Understandable / clear	3	2	4	3	4	4	2	5
B.1.3	Adequately described	3	3	4	4	4	4	2	5

Criteria / Statements		Respondents							
		SMA	MA2014	MA2015	MSSIM	MITA	ITSO	MITI&O	MEA
B.2	**Compatibility and flexibility**	**4**	**4**	**5**	**4**	**4**	**4**	**4**	**5**
B.2.1	Compatible	4	4	5	4	4	3	4	5
B.2.2	Adequate guidance provided	3	2	4	4	4	4	2	5
B.2.3	Flexible / adaptive	4	5	-	4	5	4	5	4

Table B-3 Rand Water Usability Evaluation Responses

The following are the common phrases extracted from the remarks made by the expert panel regarding the perceived usability of the Rand Water Way:

Remark Extract / Common phrases	Respondents							
	SMA	MA2014	MA2015	MSSIM	MITA	ITSO	MITI&O	MEA
Advantages and strengths								
Well-crafted / designed theory or approach.			**x**	**x**	**x**	**x**	**x**	**x**
Philosophy and principles are easy to understand.			**x**	**x**	**x**			**x**
Compatible to the organisational structure.		**x**	**x**	**x**	**x**			**x**
Compatible with the corporate governance structures.				**x**	**x**			**x**
Adaptable / flexible enough for Rand Water.	**x**	**x**		**x**	**x**		**x**	**x**
Cater for organisational growth or changes.					**x**			**x**
Disadvantages and shortcomings								
The approach is theoretical.		**x**	**x**				**x**	
The difficulty is in the implementation.	**x**	**x**				**x**	**x**	
Extra guidance required at a practical level.	**x**		**x**				**x**	
A lot of implementation effort and time required.		**x**	**x**			**x**	**x**	
Not compatible with culture in control system functions.			**x**				**x**	

Table B-4 Rand Water Usability Remarks Extract

B.2. Evaluation at Similar Organisations

The following similar organisations were used during the evaluation of the Rand Water Way:

	Org # 1	Org # 2	Org # 3
Brief description	A private global beer and soft drinks manufacturer	A state owned national postal and communication service provider	A private multi-national iron ore mining company
Industry	Manufacturing: Beverage	Logistics: Postal communications	Mining
Public / private sector	Private - Listed company JSE, LSE	Public – State owned	Private
Location / Base	United Kingdom and South Africa	Botswana	South Africa
Foot print	Global / Multi-national. 60 countries	National	Multi-national
Annual Revenue	Group: ZAR 268 billion	ZAR 400 million	ZAR 20 billion
Infrastructure asset value	ZAR 1.9 billion	ZAR 350 million	ZAR 100 billion
Number of staff	SA: 9 400	700	15 000
Digital organisation description	All IT functions report to a global CIO. Control system functions report to Manufacturing	A centralised IT function report to the CEO. Separate automated mail sorting, printing and delivery of mail/parcels function report to the CEO	IT and control system functions reporting to a global CIO
Digital landscape description	SAP ERP; Business Objects, Qlikview. Wonderware Scada, Labware LIMS, in-house custom MES (MS), RS-Batch	Microsoft, ACCPAC, Escher Web RiPoste (POS system), UPU parcel and money transfer systems. Automated mail sorting and automated printing (Pitney Bowes)	SAP ERP, ILOPS, Starlims, Hyperion, Wonderware Scada

Table B-5 Participating Organisations

	Org # 4	Org # 5	Org # 6
Brief description	A private multi-national FMCG manufacturer	A South African-based multinational platinum mining company	A South African-based multinational cement manufacturer
Industry	Manufacturer - FMCG	Mining	Manufacturing and construction
Public / private sector	Private	Private	Private
Location / Base	United Kingdom with a South Africa subsidiary	South Africa	South Africa
Foot print	Multi-national	Multinational with representation in Africa (South Africa, Zimbabwe)	Multi-national on African continent
Annual Revenue	ZAR 650 billion	Not specified	Not specified
Infrastructure asset value	ZAR 145 billion	Not specified	Not specified
Number of staff	120 000	Not specified	2,000
Digital organisation description	Global IT function and CIO. Control systems are part of Manufacturing	The group IT function reports to the Group Executive Shared Services and the group control system functions reports to the Business Unit Manager	Group IT reports to the CIO. CIO is responsible for IT components of the control systems. COO is responsible for the plant control systems.
Digital landscape description	SAP ERP, Wonderware Scada, Labware LIMS	SAP ERP, SAP BW & BO, MES – Aspen Mine Technical – MineRP; Wonderware Scada, Labware LIMS & Cclass	SAP ERP & DMS, Transvision logistics management, AES orders, Tableau BI and analytics, PPO project management, Truck Tracker vehicle tracking, ABB and Command Alkon

Table B-5 Participating Organisations (continued)

	Org # 7	Org # 8	Org # 9
Brief description	A South African subsidiary of a private soft drinks global manufacturer	South African-based metropolitan water services utility	South African-based regional water services utility
Industry	Manufacturing	Water and sanitation	Water and sanitation
Public / private sector	Private	Public	Public
Location / Base	USA	South Africa	South Africa
Foot print	Multinational. Representation in 200+ countries. Includes 16 autonomous entities	Metropolitan	Regional / Provincial, including 3 subsidiaries
Annual Revenue	ZAR 240 billion	ZAR 6,8 billion	ZAR 2,2 billion
Infrastructure asset value	ZAR 80 billion	ZAR 10 billion	ZAR 6 billion
Number of staff	20,000+	2,400	1,200
Digital organisation description	Global IT service function reports to CIO. Corporate control system function	IT department reports into the Finance Division. Control System function report into the Office of the COO	A corporate IT function reporting to a CIO. Control system environment reports to Operations. Both subsidiaries are supported by corporate IT
Digital landscape description	SAP ERP, SAP Logistics, SAP HR & SAP BI; Kronos	SAP ERP, Meter Reading Quality Control system, Water Prepayment System, Infrastructure Management Quality System, GIS, Scada and Labware (LIMS)	JD Edwards (Financials & SCM), Maximo (Assets), EDAMS,(Metering & Billing), Vision (HRM), D1 (Payroll), Esri GIS, Adroit, Scada, and Labware (LIMS)

Table B-5 Participating Organisations (continued)

The following questionnaire was used for evaluating the Rand Water Way at similar organisations:

Name of organisation	
Position(s) / Role(s) of respondent(s)	

May the name of the organisation be used in the dissertation? *(mark with an "X")*	**Yes**	**No**

If NO then a brief description of the organisation will be used. Only if all respondents respond YES, will the names of any responding organisations be used in the dissertation.

Organisational Characteristics			
Industry		**Private / Public / PPP**	
Foot Print	*(e.g. International, National, Regional, Local / Metropolitan)*	**Location**	
Annual Revenue		**Number. of staff**	
Infrastructure Asset Value		**Number of autonomous business units**	
IT Landscape	.	**Control System Landscape**	
A brief description of the digital organisation.			

The organisational characteristics will be used as an indication of the size and complexity of the organisation. If the information requested is not known or considered confidential, then please leave the space blank.

Please select the most appropriate response for each of the statements.		**Rating**				
		1 - Strongly disagree	**2 - Disagree**	**3 - Neutral**	**4 - Agree**	**5 - Strongly Agree**
Statements						
A	**Usefulness**					
A.1	**Problem relevance:** Are the statements below applicable to your organisation?					
A.1.1	**Technology and information related problems**					
1.1.1	**Digital technology size and complexity:** The digital technology landscape, including IT and control systems, is large, complex and heterogeneous.					

Please select the most appropriate response for each of the statements.		Rating				
		1 - Strongly disagree	2 - Disagree	3 - Neutral	4 - Agree	5 - Strongly Agree
Statements						
1.1.2	**Digital isolation and incompatibility:** Control systems are isolated and / or incompatible with IT systems and does not allow asset information to be exchanged between control systems and IT systems.					
1.1.3	**Fast pace of digital technology development:** Digital technology and convergence between control and IT system technology are developing at a fast pace.					
1.1.4	**Diverse asset information source:** Asset information originates and is stored across the digital landscape (control systems and IT systems).					
1.1.5	**Inconsistent asset information management:** Asset information is not managed consistently across the digital (control and IT systems) landscape (e.g. naming conventions, format, data quality, classification, ownership).					
1.1.6	**Big Data:** Asset information volume (e.g. storage size, number of data items, granular data) and variety (e.g. format, medium) is high and increasing.					
A.1.2	**Process related problems**					
1.2.1	**Security threats:** Information security threats (e.g. malicious software, unauthorized access, natural disasters) pose a risk to the overall digital landscape, especially in the case of an integrated digital landscape.					
1.2.2	**Governance maturity inconsistency:** The maturity of digital governance and operational controls differ between control and IT system functions and / or solutions.					
1.2.3	**Compliance as end goal:** The primary purpose of digital / IT governance is compliance to a standard, code or framework.					
1.2.4	**Operational control inadequacy:** The operational process controls of the control systems do not provide adequate assurance that quality data will be made available timeously for asset decision making.					
1.2.5	**Lack of alignment:** There is no alignment between the control systems and IT functions in terms of future direction and common strategic goals.					
A.1.3	**People and organisational related problems**					
1.3.1	**Organisational structure:** The control system and IT functions does not report into the same function / organisational unit.					
1.3.2	**Lack of trust:** There is a lack of trust in IT system functions by the control system functions, either in terms of capability and / or intention.					
1.3.3	**Resistance to change:** There is resistance to change by control system functions and / or IT functions.					

Please select the most appropriate response for each of the statements.		Rating				
		1 - Strongly disagree	2 - Disagree	3 - Neutral	4 - Agree	5 - Strongly Agree
Statements						
1.3.4	**Lack of collaboration and sharing:** There is a lack of collaboration, resource / skills sharing and / or communication between IT and control system functions.					
A.2	**Problem resolution** Will a contextualized version of the Rand Water Way resolve the problems relevant to your organisation?					
A.2.1	**Technology and information problem resolution**					
2.1.1	**Complexity, size and pace of change:** It will address the complexity, size and fast pace of change and convergence of the digital (control system & IT) landscape.					
2.1.2	**Asset information exchange:** It will assist in enabling asset information to be exchanged between control systems and IT systems for asset decision support (via integration and compatible technology).					
2.1.3	**Asset information fusion:** It will assist in ensuring that the required asset information from across the digital landscape is fused or harmonised to provide an integrated set of asset information in support of asset decision.					
2.1.4	**Asset data quality:** It will assist in ensuring that asset information has the required level of quality (e.g. completeness, correctness) to support effective asset decision making.					
A.2.2	**Process problem resolution**					
2.2.1	**Cyber security threats:** It will assist in ensuring that the digital / cyber security threats and risks are adequately mitigated for the integrated digital landscape.					
2.2.2	**Lack of operational controls:** It will adequately address the risk related to the lack of operational controls (e.g. change and configuration management)					
2.2.3	**Value delivery beyond compliance**: It will assist in ensuring that the governance mechanisms and operational process controls deliver value beyond compliance					
2.2.4	**Avoid over and under-regulation:** It will prevent the negative implications of over and under regulation of the digital environment.					
A.2.3	**People and organisational problem resolution**					
2.3.1	**Improve involvement and commitment:** It will ensure involvement and / or commitment from all internal stakeholders across the organisation.					
2.3.2	**Reduce resistance to change:** It will reduce and / or eliminate the resistance to this change in the way of thinking about digital governance within the organisation.					
2.3.3	**Improve trust:** It will improve the trust between the digital functions in terms of capability and / or intention.					

Please select the most appropriate response for each of the statements.		Rating				
		1 - Strongly disagree	2 - Disagree	3 - Neutral	4 - Agree	5 - Strongly Agree
Statements						
2.3.4	**Improve collaboration and sharing**: It will improve the collaboration and communication between the digital functions of the organisation, as well as the sharing or skills and expertise.					
2.3.5	**Reduce turf protection:** It will reduce the territorial behaviour of digital functions within the organisation.					
2.3.6	**Improve sustainability:** It will ensure a sustainable change in the way of thinking about digital governance across the organisation. Digital functions will continue to comply with the agreed governance mechanisms and operational controls.					
B	**Usability**					
B.1	**Simplicity and clarity**					
B.1.1	**Simple:** The philosophy and underlying principles are simple, logical and straightforward.					
B.1.2	**Understandable / clear:** It is clear and easily understandable, including the philosophy, principles, framework and the constituent parts.					
B.1.3	**Adequately described:** The approach, including its constituent parts, are adequately defined and described.					
B.2	**Compatibility and flexibility**					
B.2.1	**Compatible:** It is compatible with the organisation (e.g. organisational structure; governance structures).					
B.2.2	**Adequate guidance:** Adequate guidance is provided in terms of the contextualization for and implementation of the Rand Water Way at the organisation.					
B.2.3	**Flexible / adaptive:** It is flexible, generic and adaptable enough to be contextualized for the organisation					

The statements in the problem relevance section are stated in the present tense as it defines the current situation at the organisation. The statements in the resolution section are stated in future tense as it is evaluating whether the Rand Water Way will / could potentially resolve the relevant problem, if it is contextualised and implemented at the organisation.

The responses received from the expert panel members regarding the ***potential perceived usefulness*** of the Rand Water Way are as follows:

Criteria / Statements		Respondents								
		Org # 1	**Org # 2**	**Org # 3**	**Org # 4**	**Org # 5**	**Org # 6**	**Org # 7**	**Org # 8**	**Org # 9**
A	**Usefulness**	**4**	**5**	**4**	**4**	**4**	**4**	**4**	**4**	**4**
A.1	**Problem relevance**	**4**	**4**	**3**	**4**	**4**	**3**	**4**	**4**	**4**
A.1.1	**Technology and information problems**	**5**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**5**
1.1.1	Digital technology size and complexity	5	3	5	4	5	5	4	4	4
1.1.2	Digital isolation and incompatibility	4	4	2	4	3	2	5	2	4
1.1.3	Fast pace of digital technology development	5	4	4	4	4	4	4	2	5
1.1.4	Diverse asset information sources	5	5	4	4	5	4	4	5	5
1.1.5	Inconsistent asset information management	4	5	2	2	4	2	4	4	5
1.1.6	Big data (volume, variety)	5	5	5	4	4	4	3	5	4
A.1.2	**Process problems**	**4**	**5**	**3**	**3**	**4**	**2**	**3**	**4**	**4**
1.2.1	Security threats	5	5	4	5	4	5	5	4	5
1.2.2	Governance maturity inconsistency	3	5	4	4	4	2	4	5	4
1.2.3	Compliance as end goal	4	5	2	2	5	2	2	4	3
1.2.4	Operational control inadequacy	4	5	2	3	4	1	2	4	2
1.2.5	Lack of alignment	4	4	2	2	3	1	2	5	4
A.1.3	**People and organisational problems**	**4**	**4**	**4**	**4**	**3**	**2**	**4**	**4**	**4**
1.3.1	Organisational structure	4	5	5	4	5	5	5	5	5
1.3.2	Lack of trust (between digital functions)	4	2	4	3	2	1	2	4	4
1.3.3	Resistance to change	3	2	4	4	2	4	4	2	4
1.3.4	Lack of vision and/or urgency to change	5	4	3	4	3	1	2	2	4
1.3.5	Lack of change forum / coalition	4	4	2	3	3	1	4	4	4
1.3.6	Lack of collaboration and sharing	3	4	4	4	2	1	4	4	4
A.2	**Problem resolution**	**4**	**5**	**4**	**3**	**4**	**4**	**3**	**4**	**4**
A.2.1	**Technology and information problems resolution**	**4**	**5**	**4**	**3**	**4**	**5**	**4**	**4**	**5**
2.1.1	Complexity, size and pace of change	3	4	4	2	4	4	3	4	5
2.1.2	Asset information exchange	4	5	3	3	4	5	4	4	5
2.1.3	Asset information fusion	4	4	4	3	4	4	4	4	5
2.1.4	Asset data quality	4	5	4	3	4	5	4	3	5
A.2.2	**Process problems resolution**	**4**	**5**	**4**	**3**	**4**	**5**	**4**	**4**	**4**
2.2.1	Cyber security threats	5	5	3	3	4	5	5	4	4
2.2.2	Lack of operational controls	4	5	4	3	4	5	3	5	4
2.2.3	Value delivery beyond compliance	4	4	4	3	4	4	3	4	4
2.2.4	Avoid over and under-regulation	4	4	4	3	4	4	3	4	5
A.2.3	**People and organisational problems resolution**	**4**	**5**	**4**	**3**	**3**	**4**	**3**	**4**	**4**
2.3.1	Improve involvement and commitment	4	5	4	3	3	4	2	3	4
2.3.2	Reduce resistance to change	4	5	3	3	3	4	2	3	3
2.3.3	Improve trust (between digital functions)	4	5	4	3	3	4	4	4	4
2.3.4	Improve collaboration and sharing	4	5	3	3	4	4	5	4	4
2.3.5	Shared vision and direction	4	5	4	4	3	4	3	4	5
2.3.6	Sustainability of change	4	5	5	4	3	4	3	4	4

Table B-6 Detailed Similar Organisation Usefulness Evaluation Responses

The following are the ***common phrases*** extracted from the remarks made by the expert panel regarding the ***potential perceived usefulness*** of the Rand Water Way, as well as the percentage of expert panel members that made these remarks:

Remark extracts / Common phrases	% of Respondents
Advantages and strengths	
Technology has changed and/or is still changing.	56%
Is adaptable, scalable, replicatable and flexible.	56%
Is a well balanced approach.	56%
Is a practical approach.	56%
Synergies are being exploited in aligning IT and process control.	44%
Improves process maturity in IT and process control systems.	44%
Aligns strategy between all digital functions.	44%
Is applicable to organisations with large separate spheres of technologies with digital interconnectedness.	33%
Getting digital functions to work together and talk to one another.	33%
Allowing operational freedom to make decisions, whilst ensuring compliance.	33%
The underlying supporting framework is applicable, even if the industries are different.	33%
Addresses both governance and operational control.	22%
A long term approach that is not a rushed implementation.	22%
Achieving short term value.	22%
Leads to efficiency.	22%
A simple, clear and pragmatic approach to resolving issues of the digital organisation.	22%
Is a good foundation to 'sell' or market the change and to obtain buy-in.	22%
Applicable in this era of digitisation.	22%
Could save other entities time and resources to implement a similar approach.	22%
Disadvantages or shortcomings	
Standards, architecture, instrumentation and vendors vary greatly between plants and countries.	33%
Require a lot of influencing.	33%
It puts a lot of pressure on IT to deliver a solution that needs buy-in from other departments.	33%
Not utilising performance management and KPIs for ensuring sustainable change and effective execution.	33%
IT is seen as leading the Rand Water Way, instead of an executive.	22%

Table B-7 Similar Organisation Usefulness Remarks Extract

The responses received from the expert panel members regarding the ***potential perceived usability*** of the Rand Water Way are as follows:

Criteria / Statements		Respondents								
		Org # 1	**Org # 2**	**Org # 3**	**Org # 4**	**Org. # 5**	**Org. # 6**	**Org # 7**	**Org # 8**	**Org # 9**
B	**Usability**	**4**	**4**	**3**	**3**	**3**	**5**	**4**	**4**	**4**
B.1	**Simplicity and clarity**	**4**	**4**	**3**	**3**	**3**	**5**	**4**	**5**	**5**
B.1.1	Simple	4	4	2	4	3	5	4	5	4
B.1.2	Understandable / clear	4	4	3	3	3	5	4	5	5
B.1.3	Adequately described	4	4	3	2	3	5	4	4	4
B.2	**Compatibility and flexibility**	**3**	**4**	**4**	**3**	**3**	**5**	**4**	**4**	**4**
B.2.1	Compatible	3	4	4	2	3	5	3	4	3
B.2.2	Adequate guidance provided	2	4	4	4	3	5	4	3	4
B.2.3	Flexible / adaptive	3	4	4	2	3	5	4	4	4

Table B-8 Detailed Similar Organisation Usability Evaluation Responses

The following are the ***common phrases*** extracted from the remarks made by the expert panel regarding the ***potential perceived usability*** of the Rand Water Way, as well as the percentage of expert panel members that made these remarks:

Remark extracts / Common phrases	% of Respondents
Advantages and strengths	
Is adaptable, scalable, replicatable and flexible.	67%
The roadmap is well thought through, clear and logical.	56%
The underlying supporting framework is applicable, even if the industries are different.	44%
The approach is well documented and detailed.	44%
Could save other entities time and resources to implement a similar approach.	22%
Disadvantages or shortcomings	
Will need extensive tailoring for multinational organisations.	22%
Must be developed further for adaptation to multiple forms of organisations.	22%
Need more guidance in terms of how to implement the roadmap.	22%

Table B-9 Similar Organisation Usability Remarks Extract

English Summary

Organisations and countries are globally relying on infrastructure investment and the performance of existing ***infrastructure assets,*** to improve economic growth and the quality of life of citizens. Infrastructure asset management aims to address the lack of timely investment in infrastructure and the inadequate maintenance of existing infrastructure assets. Evidence-based strategic asset management decision making is at the core of infrastructure asset management. It requires relevant and harmonised quality asset information from IT systems and control systems.

A number of ***real-world problems*** were identified that could prevent the successful enablement and support of strategic infrastructure asset management decision making in a sustainable manner. These problems relate to: 1) the collection and transformation of asset information into useful and reliable evidence for asset decision making; and 2) the implementation of a sustainable change in asset information management and digital governance. The problems extracted from the base, Rand Water, and generalised through literature review, include: 1) the ever increasing size and complexity of digital technology and asset data; 2) digital technology incompatibility and isolation; 3) information security threats, due to the integration of IT and control systems; 4) inadequate digital governance of control system environments; 5) the inconsistent maturity of digital governance between the IT and control system environments; 6) inadequate assurance, due a pure compliance objective; 7) the organisational segregation of IT and control system functions in large and complex infrastructure asset intensive organisations; and 8) resistance to change by digital functions.

A ***new way*** of thinking, working, controlling and modelling was required, in relation to digital governance and asset information management, in order to resolve these problems. An appropriate approach was also required to implement the new way of asset information management and digital governance in a sustainable manner for a large complex heterogeneous organisation, such as Rand Water. This research applied a recognised, appropriate and rigorous research approach. The researcher is a reflective practitioner whose reflections induced the artefact (i.e. the Rand Water Way) that was designed for, and instantiated at, the base case. Design science was used as a research philosophy and a pragmatic epistemological stance was adopted. The design science research philosophy was effectuated with the inductive-hypothetic research strategy, in order to formulate and test a tentative hypothesis (i.e. the Rand Water Way

design). The acceptance of the Rand Water Way was tested by illustrating its usage, as well as evaluating its perceived usefulness and usability.

Rand Water is the base case for this research. It is the largest water utility in Africa and provides more than 12 million people in the economic heartland of South Arica with 4,183 Ml/d of world-class potable water. Its source of raw water is 70 kilometer (44 miles) away from the bulk of the consumers. The water must also be lifted 366 meters from the source to its destination. One of Rand Water's key characteristics is its dependence on its infrastructure assets. The replacement value of the infrastructure assets is ZAR 80 billion. The aging infrastructure of Rand Water is one of its key risks. Rand Water plans to spend ZAR 13 billion on its infrastructure between 2015 and 2019. The management of infrastructure assets is a key success factor of the organisation in the achievement of agreed service levels with customers. The digital environment of Rand Water includes both IT systems (e.g. ERP) and control systems (e.g. SCADA, LIMS). The digital functions are segregated. There is one corporate IT function and two control system functions.

Some of the key ***observations from literature*** that influenced the design of the Rand Water Way are: 1) infrastructure asset management is becoming more formalised and sophisticated, which increases the need for quality asset information to make asset decisions; 2) the management of information includes related disciplines and activities, such as information security and information governance; 3) the risk of digital technology incompatibility is decreasing, but enterprise architecture remains an important discipline to manage complexity and change in an organisation; 4) it is unclear to what extent IT governance has been applied in asset intensive organisations or to control system environments; 5) there is a trend to define and implement internal IT governance frameworks, by tailoring one or more commercially available frameworks based on the characteristics of the organisation; 6) compliance to a standard or legislation is an important and common reason for organisations to implement IT governance; 7) there is a trend to follow an holistic approach to IT governance, that addresses both governance and operational level processes and controls; 8) it is recognised that the implementation of IT governance is a change initiative, rather than a technology initiative; 9) a successful implementation approach makes use of associated disciplines and mechanisms, such as project management, maturity models and transition roadmaps; and 10) implementation approaches are tailored for the specific discipline and organisation to ensure a successful transition during the long and difficult road.

The ***artefact,*** namely ***the Rand Water Way***, is an integrated enterprise-wide approach for the governance and management of asset information and the associated underlying digital technology, including IT and control systems. It is also an approach to introduce and implement this new way of thinking, working, controlling and modelling at an infrastructure asset intensive organisation. The overall ***philosophy*** of the Rand Water Way is that effective infrastructure asset management requires asset information to be managed, governed and utilised as an enterprise-wide resource. This requires: 1) an enterprise-wide digital architecture and related standards; 2) an optimal degree of enterprise-wide digital governance and operational process controls; and 3) the implementation of this new way of thinking, working, controlling and modelling in relation to asset information management and digital governance, in a sustainable manner. The Rand Water Way embodies this philosophy through its five overlapping and integrated ***constituent parts.*** These are: 1) strategy - to obtain formal commitment for the approach and to direct the rest of the constituent parts; 2) information management - the management of asset information from IT and control systems as a valuable enterprise resource; 3) architecture - the enterprise-wide digital architecture and standards related to asset information and digital technology; 4) governance - the integrated, appropriate and enterprise-wide digital governance and operational process controls for asset information and digital technology; and 5) transition management - the approach for introducing and implementing the change in a sustainable manner.

The Rand Water Way was ***operationalised and is currently being used in practice*** at Rand Water. The Rand Water Way was ***instantiated*** by: 1) contextualising it based on the Rand Water characteristics; 2) obtaining acceptance and approval from the authorised governance structures; and 3) implementing it across the three digital functions of the organisation. A co-created strategy was formalised and approved by the board of Rand Water. An enterprise architecture was created, that included IT and control systems. An enterprise information management framework was created and applied to asset information from across the digital landscape. An enterprise-wide digital governance framework was established and integrated into the corporate governance framework. The appropriate digital governance mechanisms and operational process controls were selected and prioritised, based on the result of a risk assessment. The transition roadmap was defined and implemented, in order to implement the changes mentioned above. Rand Water received value from this implementation in terms of: 1) improved digital security; 2) improved collaboration between digital functions; 3) cost savings by exploiting the convergence in technology; 4) a cost effective digital governance

solution that effectively mitigates the related risks; and 5) the ability to integrate asset information from IT and control systems on a continuous basis, and in a safe and secure manner.

The ***acceptance*** of the Rand Water Way was tested at Rand Water and at nine similar organisations from the mining, water, manufacturing and logistics industries. The perceived usefulness and usability of the Rand Water Way was evaluated at Rand Water. The potential perceived usefulness and usability, of a contextualised Rand Water Way approach, was evaluated at the nine similar organisations. The evaluation at the similar organisations tested: 1) the degree of generalisability of the Rand Water Way; and 2) the acceptance of the Rand Water Way for organisations that are at least as large and complex as Rand Water. The ***result of the evaluation was positive*** for both the Rand Water evaluation and the evaluation at the nine similar organisations. The results showed that: 1) the problems originally extracted from the base case and generalised from literature, are prevalent at large and complex infrastructure asset intensive organisations across different industries; 2) the Rand Water Way is useful to Rand Water, because it effectively addressed their problems and delivered value; 3) the Rand Water Way has been adequately generalised, in order for a contextualised version to potentially be useful to large and complex infrastructure asset intensive organisations across different industries; and 4) the Rand Water Way is "easy to use" by, and appropriate for, asset intensive organisations across different industries. However, some of the large multi-national manufacturing and mining organisations in the private sector indicated that: 1) some of the generalised problems are not relevant to their organisations anymore; and 2) a significant degree of contextualisation is required, in order for the Rand Water Way to be useful to them.

The research ***contributes to descriptive knowledge*** by increasing the knowledge and understanding of: 1) the associated problem domain; and 2) the relevant concepts and theories related to the research. It ***contributes to theory and prescriptive knowledge*** related to the field of information management and digital governance, as applied to large and complex infrastructure asset intensive organisations. This was achieved through the design and instantiation of an identifiable and unique artefact, namely the Rand Water Way, as the answer to the two research questions. The Rand Water Way is a ***unique artefact***. It addresses the gap in literature regarding: 1) digital governance in control system environments; 2) enterprise-wide digital governance for industrial organisations that includes IT and control systems; and 3) an approach to implement enterprise-wide digital governance in a large complex infrastructure asset intensive organisation. The Rand Water Way goes beyond IT governance,

IT management, information management and compliance to any specific standard, code or framework. The uniqueness of the Rand Water Way is primarily in its integration and encapsulation of the individual concepts and theories into a single integrated approach, that focuses on digital governance in support of strategic infrastructure asset decision making in large and complex infrastructure asset intensive organisations. Each of the integrated constituent parts are required to make its contribution to the holistic solution of the problems. Some of the specific unique characteristics of the Rand Water Way include: 1) a two-tier hierarchy for the prioritisation of controls, consisting of an essential centralised controls tier and an important federated controls tier; and 2) a flexible transition roadmap, consisting of continuous phases that focuses first on building trust, secondly on exploiting efficiency improvement opportunities at an acceptable level of risk, and finally on formalisation of the digital environment.

The research also provides direction regarding ***future research***. Examples of these are: 1) the adaptation, contextualisation and instantiation of the Rand Water Way, in order to address the information management and digital governance related problems being experienced by multi-national organisations with autonomous or semi-autonomous business units, each with their own infrastructure installations; and 2) the design and instantiation of an infrastructure asset management decision enhancement studio, focusing on strategic infrastructure asset management decisions for large and complex infrastructure asset intensive organisations, enabled by the Rand Water Way as a foundation.

Afrikaanse Samevatting

Organisasies en regerings maak wêreldwyd staat op infrastruktuur investering en die prestasie van bestaande ***infrastruktuur bates***, om ekonomiese groei en die lewensgehalte van landsburgers te verbeter. Hierdie infrastruktuur sluit kritieke nasionale installasies in, soos byvoorbeeld: water en sanitasie, gesondheid, verdediging en energie. Infrastruktuur bate bestuur is daarop gemik om die tekort aan tydige investering in infrastruktuur, en die onvoldoende instandhouding van bestaande infrastruktuur bates, aan te spreek. Strategiese bate bestuur besluitneming, wat op voldoende bewyse gebaseer is, is die kern van infrastruktuur bate bestuur. Dit vereis toepaslike en geharmoniseerde gehalte bate inligting van beide inligting tegnologie (IT) stelsels en industriële beheer stelsels.

ŉ Aantal ***praktiese en werklike probleme*** is geïdentifiseer, wat die volgehoue suksesvolle ondersteuning van strategiese infrastruktuur bate bestuur besluitneming kan verhoed. Hierdie probleme hou verband met: 1) die versameling en omvorming van infrastruktuur bate inligting in bruikbare en betroubare bewyse, ter ondersteuning van besluitneming; en 2) die inwerking stelling van ŉ volhoubare verandering, in terme van inligting bestuur en digitale beheer praktyke. Die probleem uittreksel vanuit die basis geval (Rand Water), wat deur middel van literatuuroorsig veralgemeen is, sluit die volgende in: 1) die immer-groeiende grootte en ingewikkeldheid van digitale tegnologie en infrastruktuur bate inligting; 2) digitale tegnologie isolasie en onverenigbaarheid; 3) inligting sekuriteit verwante bedreigings, as gevolg van die integrasie van IT en industriële beheer stelsels; 4) onvoldoende digitale beheer oor industriële beheer stelsels; 5) die inkonsekwente toepassing en mate van formalisering van digitale beheer tussen die IT en industriële beheer stelsel omgewings; 6) onvoldoende waarborge, as gevolg van die najaag van suiwere nakomingsdoelwitte, ten opsigte van digital beheer; 7) die organisatoriese skeiding van IT funksies en industriële beheer stelsel funksies in groot en ingewikkelde infrastruktuur-intensiewe organisasies; en 8) weerstand deur digitale funksies teen enige verandering.

ŉ ***Nuwe wyse*** ten opsigte van dink, werk, beheer en modellering was nodig vir digitale beheer en infrastruktuur bate inligting bestuur, ten einde hierdie probleme aan te spreek. ŉ Toepaslike benadering was ook nodig om die nuwe manier van bate inligting bestuur en digitale beheer vir ŉ groot en ingewikkelde heterogene organisasie, soos Rand Water, inwerking te stel. Hierdie navorsing het ŉ erkende, toepaslike en streng navorsing benadering toegepas.

Die navorser is ŉ reflekterende praktisyn wat besin oor ŉ produk (die Rand Water Wyse), wat by die basis geval ontwerp en inwerking gestel is. Ontwerp wetenskap is gebruik as navorsing filosofie, en ŉ pragmatiese epistemologiese benadering is gevolg. Uitvoering is aan die ontwerp wetenskap navorsing filosofie gegee, deur middel van ŉ induktiewe-hipotetiese navorsing strategie, ten einde ŉ hipotese (d.i. die Rand Water Wyse) te ontwerp en te toets. Die aanvaarding van die Rand Water Wyse is getoets aan die hand van sy gebruik, asook ŉ evaluasie van sy waargenome nuttigheid en bruikbaarheid.

Rand Water is die basis geval vir hierdie navorsing. Dit is die grootste water verskaffer in Afrika. Meer as 12 miljoen mense, in die ekonomiese middelpunt van Suid-Afrika, word daagliks van 4 183 Ml wêreld gehalte water voorsien. Die waterbron is 70 kilometer vanaf die meerderheid van verbruikers geleë. Die water moet ook met 366 meter vanaf die bron tot by die eindbestemming gelig word. Een van Rand Water se uitstaande kenmerke, is sy afhanklikheid van sy infrastruktuur bates. Die vervangingswaarde van die infrastruktuur bates is ZAR 80 miljard. Die verouderende infrastruktuur is een van Rand Water se hoof risiko's. Rand Water beplan om tussen 2015 en 2019, ZAR 13 miljard aan sy infrastruktuur te spandeer. Die bestuur van infrastruktuur bates is ŉ sleutel sukses faktor vir die organisasie, ten einde ooreengekome diensleweringsvlakke met sy verbruikers te verseker. Die digitale omgewing van Rand Water sluit IT en industriële beheer stelsels (bv. SCADA, LIMS) in. Daar is een korporatiewe IT funksie en twee industriële beheer stelsel funksies. Hierdie digitale funksies is organisatories van mekaar geskei.

Die ***sleutel waarnemings vanuit die literatuur,*** wat ŉ invloed op die ontwerp van die Rand Water Wyse gehad het, is die volgende: 1) infrastruktuur bate bestuur is besig om meer geformaliseer en gesofistikeerd te raak, wat die behoefte verhoog vir gehalte infrastruktuur bate inligting om bate bestuur besluite te neem; 2) die bestuur van inligting sluit verwante dissiplines en aktiwiteite in, soos inligting sekuriteit en inligting beheer; 3) die risiko van digitale tegnologie isolasie en onverenigbaarheid is besig om te verminder, maar ondernemingsargitektuur bly ŉ belangrike dissipline, ten einde die ingewikkelheid van, en verandering in, ŉ organisasie te bestuur; 4) dit is onduidelik tot welke mate IT beheer in industriële infrastruktuur-intensiewe organisasies aangewend is; 5) daar is ŉ neiging om interne IT beheer raamwerke te ontwerp en inwerking te stel, deur een of meer kommersieël beskikbare raamwerke aan te pas, gebaseer op die unieke eienskappe van die organisasie; 6) nakoming van ŉ standaard of wetgewing is ŉ belangrike en algemene rede vir organisasies om IT beheer inwerking te stel; 7) daar is ŉ neiging om ŉ holistiese benadering te volg, ten opsigte van IT

beheer, wat beide beheer en bedryfsvlak proses kontroles aanspreek; 8) dit word erken en aanvaar dat die inwerking stelling van IT beheer ŉ verandering inisiatief is, eerder as ŉ suiwere tegnologie inisiatief; en 9) inwerking stelling benaderings word vir die spesifieke dissipline en organisasie aangepas, ten einde ŉ suksesvolle oorgang te bewerkstellig.

Die ***produk***, naamlik die **Rand Water Wyse**, is ŉ geïntegreerde ondernemingswye benadering ten opsigte van die beheer en bestuur van infrastruktuur bate inligting en die onderliggende digitale tegnologie. Dit sluit beide IT en industriële beheer stelsels in. Dit is ook ŉ benadering om hierdie nuwe wyse van dink, werk, beheer en modellering by ŉ infrastruktuur bate-intensiewe organisasie inwerking te stel. Die oorhoofse ***filosofie*** van die Rand Water Wyse is dat doeltreffende infrastruktuur bate bestuur vereis dat bate inligting as ŉ ondernemingswye hulpmiddel bestuur, beheer en gebruik word. Dit vereis weer die volgende: 1) ŉ ondernemingswye digitale argitektuur en verwante standaarde; 2) ŉ optimale mate van ondernemingswye digitale beheer en bedryfsvlak proses kontroles; en 3) die inwerking stelling van hierdie nuwe wyse van dink, werk, beheer en modellering, met betrekking tot inligting bestuur en digitale beheer, op ŉ volhoubare manier. Die Rand Water Wyse omvat hierdie filosofie, deur middel van sy vyf oorvleuelende en geïntegreerde ***saamgestelde dele.*** Hierdie saamgestelde dele is: 1) strategie – om formele goedkeuring en ondersteuning van die uitvoerende bestuur vir die benadering te verkry, en om rigting aan die res van die saamgestelde dele te gee; 2) inligting bestuur – die bestuur van infrastruktuur bate inligting, van beide IT en industriële beheer stelsels, as ŉ waardevolle ondernemingswye hulpmiddel; 3) argitektuur – die ondernemingswye digitale argitektuur en standaarde, wat verband hou met infrastruktuur bate inligting en die verwante digitale tegnologie; 4) beheer – die geïntegreerde, toepaslike en ondernemingswye digitale beheer en bedryfsvlak proses kontroles vir infrastruktuur bate inligting en verwante digitale tegnologie; en 5) oorgang bestuur – die oorgang bestuur benadering vir die inwerking stelling van die verandering in denk wyse en werkswyse op ŉ volhoubare manier.

Die Rand Water Wyse is ***inwerking gestel en word tans in die praktyk gebruik*** by Rand Water. Dit is bereik deur: 1) die Rand Water Wyse te kontekstualiseer en aan te pas, gebaseer op Rand Water se eienskappe; 2) aanvaarding en goedkeuring te verkry van die relevante beheer strukture; en 3) dit regoor die drie digitale funksies van die organisasie van toepassing te maak. ŉ Gesamentlike digitale strategie is geformaliseer, en deur die raad van Rand Water goedgekeur. ŉ Ondernemingswye argitektuur is geskep, wat IT en industriële beheer stelsels insluit. ŉ Ondernemingswye inligting bestuur raamwerk is geskep en op infrastruktuur bate

inligting van beide IT and industriële beheer stelsels toegepas. ’n Ondernemingswye digitale beheer raamwerk is inwerking gestel, en in die korporatiewe beheer raamwerk geïnkorporeer. Die toepaslike digitale beheer meganismes en bedryfsvlak proses kontroles is gekies en geprioritiseer, op grond van die uitslag van ’n risiko ontleding. Die oorgang padkaart is bepaal en gebruik, ten einde die veranderings hierbo genoem, inwerking te stel. Rand Water het waarde uit hierdie verandering gerkry, ten opsigte van die volgende: 1) verbeterde digitale sekuriteit; 2) verbeterde samewerking tussen digitale funksies; 3) koste besparings, as gevolg van die samestroming en integrasie van digitale tegnologie; 4) ’n koste-doeltreffende digitale beheer oplossing, wat die verwante risiko’s doeltreffend verminder; en 5) die vermoë om infrastruktuur bate inligting van IT en industriële beheer stelsels, op ’n voortdurende basis en veilige wyse, te integreer.

Die ***aanvaarding*** van die Rand Water Wyse is getoets by Rand Water en nege soortgelyke organisasies in die mynbou, water, vervaardiging en logistieke bedrywe. Die waargenome nuttigheid en bruikbaarheid van die Rand Water Wyse is deur Rand Water geëvalueer. Die potensiële waargenome nuttigheid en bruikbaarheid van ’n gekontekstualiseerde Rand Water Wyse, is vir die nege soortgelyke organisasies geëvalueer. Die evaluasie by die soortgelyke organisasies het die volgende getoets: 1) die mate van veralgemening van die Rand Water Wyse; en 2) die aanvaarding van die Rand Water Wyse vir organisasies wat ten minste so groot en ingewikkeld as Rand Water is. Die ***uitslag van die evaluasie was positief*** vir beide die Rand Water evaluasie en die evaluasie by die nege soortgelyke organisasies. Die uitslae het getoon dat: 1) die probleme van die basis geval, wat deur middel van literatuuroorsig veralgemeen is, ook by ander groot en ingewikkelde infrastruktuur bate-intensiewe organisasies in verskillende bedrywe voorkom; 2) die Rand Water Wyse nuttig is vir Rand Water, aangesien dit hulle probleme doeltreffend aanspreek en waarde toevoeg; 3) die Rand Water Wyse genoegsaam veralgemeen is, deurdat ’n gekontekstualiseerde weergawe vir groot en ingewikkelde infrastruktuur bate-intensiewe organisasies in verskeie nywerhede potensieël nuttig is; en 4) die Rand Water Wyse maklik is om te gebruik en toepaslik is vir infrastruktuur bate-intensiewe organisasies in verskeie nywerhede. Sommige van die groot multi-nasionale vervaardiging en mynbou organisasies in die privaat sektor, het egter aangedui dat: 1) van die veralgemeende probleme nie meer op hulle organisasies van toepassing is nie; en 2) ’n beduidende mate van kontekstualisering van die Rand Water Wyse nodig is om vir hulle van nut te wees.

Die navorsing ***dra by tot beskrywende kennis,*** deur middel van die vermeerdering van kennis oor, en begrip van: 1) die verwante probleem terrein; en 2) die begrippe en teorieë wat met die navorsing verband hou. Dit ***dra ook by tot teorie en voorskriftelike kennis,*** wat verband hou met die terrein van inligting bestuur en digitale beheer, soos wat dit in groot en ingewikkelde infrastruktuur bate-intensiewe organisasies toegepas word. Hierdie bydra is bereik deur die ontwerp en inwerking stelling van ŉ identifiseerbare en unieke produk, naamlik die Rand Water Wyse, wat dien as antwoord op die twee navorsingsvrae. Die Rand Water Wyse is ŉ ***unieke produk.*** Dit spreek die volgende gapings in die literatuur aan: 1) digitale beheer in industriële beheer stelsel omgewings; 2) ondernemingswye digitale beheer vir industriële organisasies, wat IT en industriële beheer stelsels insluit; en 3) ŉ benadering om ondernemingswye digitale beheer in ŉ groot en ingewikkelde infrastruktuur bate-intensiewe organisasie inwerking te stel. Die Rand Water Wyse gaan verder as tipise IT beheer, IT bestuur, inligting bestuur en die nakoming van enige spesifieke wet, standaard, kode of raamwerk. Die primêre uniekheid van die Rand Water Wyse is te vinde in sy integrasie en omsluiting van die individuele begrippe en teorieë, in ŉ enkele geïntegreerde benadering, wat fokus op digitale beheer, ten einde strategiese infrastruktuur bate besluitneming in groot en ingewikkelde infrastruktuur bate-intensiewe organisasies te ondersteun. Elk van die vyf geïntegreerde saamgestelde dele word benodig om by te dra tot die holistiese oplossing van die probleme. Die spesifieke unieke eienskappe van die Rand Water Wyse, sluit in: 1) ŉ tweevlakkige hiërargie vir die prioritisering van beheer meganismes, wat bestaan uit ŉ noodsaaklike gesentraliseerde beheer meganisme vlak en ŉ belangrike federale beheer meganisme vlak; en 2) ŉ buigsame oorgang padkaart wat bestaan uit deurlopende fases, wat eerstens fokus op die verbetering van vertroue tussen die digital funksies, tweedens op die benutting van doeltreffendheid verbetering geleenthede met ŉ aanvaarbare mate van risiko, en laastens op formalisering van die digitale omgewing van die organisasie.

Hierdie navorsing verleen homself toe tot ***toekomstige navorsing***. Voorbeelde hiervan is: 1) die aanpassing, kontekstualisering en inwerking stelling van die Rand Water Wyse, ten einde die inligting bestuur en digitale beheer verwante probleme aan te spreek, wat ervaar word deur multi-nasionale organisasies met outonome of semi-outonome besigheid eenhede, elk met sy eie infrastruktuur installasies; en 2) die ontwerp en inwerking stelling van ŉ infrastruktuur bate bestuur besluitneming verbetering studio, wat fokus op strategiese infrastruktuur bate bestuur besluite vir groot en ingewikkelde infrastruktuur bate-intensiewe organisasies, wat deur die Rand Water Wyse ondersteun word.

Researcher Resume

Thinus Bekker has more than 25 years of experience in the ICT arena in the financial, logistics, telecommunications and water utility industries. This includes experience in private and state-owned enterprises. He also has experience in non-ICT areas, such as business process management, project and program management, facilities management, risk management, records management and knowledge management. Thinus holds a Master's degree, PMP certification and ITIL Foundation certification. He is a member of the Institute of Directors of South Africa, Project Management South Africa, the Institute of Information Technology Professionals South Africa, and an associate member of the Government IT Officers Council. At the time of this research, Thinus was the General Manager IT & Knowledge Management at Rand Water, fulfilling the role of a Chief Information Officer.